JUL 11 1986
COMPLETED 69/4. J89/2 :S.hrg.99-639

S. HRG. 99-639

COMPUTER FRAUD LEGISLATION

S.194 ORIGINAL

HEARING

BEFORE THE

SUBCOMMITTEE ON CRIMINAL LAW

OF THE

COMMITTEE ON THE JUDICIARY

UNITED STATES SENATE

NINETY-NINTH CONGRESS

FIRST SESSION

ON

S. 440

A BILL TO AMEND TITLE 18, UNITED STATES CODE, TO CREATE AN OFFENSE FOR THE USE, FOR FRAUDULENT OR OTHER ILLEGAL PURPOSES, OF ANY COMPUTER OWNED OR OPERATED BY CERTAIN FINANCIAL INSTITUTIONS AND ENTITIES AFFECTING INTERSTATE COMMERCE

AND

S. 1678

A BILL TO AMEND TITLE 18, UNITED STATES CODE, TO PROTECT THE USE OF FEDERAL COMPUTER SYSTEMS AGAINST FRAUD AND ABUSE

OCTOBER 30, 1985

Serial No. J-99-70

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE

58-745 O WASHINGTON : 1986

For sale by the Superintendent of Documents, Congressional Sales Office
U.S. Government Printing Office, Washington, DC 20402

I

BEST COPY AVAILABLE

COMMITTEE ON THE JUDICIARY

STROM THURMOND, South Carolina, *Chairman*

CHARLES McC. MATHIAS, JR., Maryland
PAUL LAXALT, Nevada
ORRIN G. HATCH, Utah
ALAN K. SIMPSON, Wyoming
JOHN P. EAST, North Carolina
CHARLES E. GRASSLEY, Iowa
JEREMIAH DENTON, Alabama
ARLEN SPECTER, Pennsylvania
MITCH McCONNELL, Kentucky

JOSEPH R. BIDEN, JR., Delaware
EDWARD M. KENNEDY, Massachusetts
ROBERT C. BYRD, West Virginia
HOWARD M. METZENBAUM, Ohio
DENNIS DECONCINI, Arizona
PATRICK J. LEAHY, Vermont
HOWELL HEFLIN, Alabama
PAUL SIMON, Illinois

DENNIS W. SHEDD, *Chief Counsel and Staff Director*
DEBORAH K. OWEN, *General Counsel*
DEBORAH G. BERNSTEIN, *Chief Clerk*
MARK H. GITENSTEIN, *Minority Chief Counsel*

SUBCOMMITTEE ON CRIMINAL LAW

PAUL LAXALT, Nevada, *Chairman*

STROM THURMOND, South Carolina
ARLEN SPECTER, Pennsylvania
CHARLES McC. MATHIAS, JR., Maryland

JOSEPH R. BIDEN, JR., Delaware
EDWARD M. KENNEDY, Massachusetts
HOWARD M. METZENBAUM, Ohio

WILLIAM S. MILLER, JR., *Chief Counsel and Staff Director*

BEST COPY AVAILABLE

CONTENTS

Opening Statements

	Page
Laxalt, Senator Paul	1
Thurmond, Chairman Strom	24

Proposed Legislation

S. 440—Computer Systems Protection Act of 1985	3
S. 1678—Federal Computer Systems Protection Act of 1985	11

Chronological List of Witnesses

Trible, Hon. Paul S., Jr., a U.S. Senator from the State of Virginia	16
Toensing, Victoria, Deputy Assistant Attorney General, Criminal Division, Department of Justice	25
Petty, William G., commonwealth attorney for the city of Lynchburg, VA, on behalf of the National District Attorney's Association	39
Sponski, John J., group executive officer, Sovran Bank; Philip M. Walker, general regulatory counsel, GTE Telenet Inc.; and Norbert J. Kubilus, vice president, educational testing service, Lawrence Township, NJ	50

Alphabetical Listing and Materials Submitted

Kubilus, Norbert J.:	
Testimony	57
Prepared statement	60
Petty, William G.:	
Testimony	39
Prepared statement	45
Sponski, John J.: Testimony	50
Toensing, Victoria:	
Testimony	25
Prepared statement	29
Trible, Hon. Paul:	
Testimony	16
Statement of Walter R. Kurth, president, Associated Credit Bureau, Inc.	20
Walker, Philip M: Testimony	54

BEST COPY AVAILABLE

COMPUTER FRAUD LEGISLATION—S. 440 AND S. 1678

WEDNESDAY, OCTOBER 30, 1985

U.S. SENATE,
SUBCOMMITTEE ON CRIMINAL LAW,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:05 a.m., in room SD-226, Dirksen Senate Office Building, Hon. Paul Laxalt (chairman of the subcommittee) presiding.

Also present: Senators Thurmond, Specter, and Trible (ex officio).

Staff present: William Miller, majority counsel; Michael Wootten, counsel; Scott Green, minority counsel; and Darren Trigonoplos, legislative aide to Senator Trible.

OPENING STATEMENT OF SENATOR PAUL LAXALT

Senator LAXALT. The subcommittee will come to order.

I want to welcome all of you to this subcommittee hearing on Senate bill 440, Senate bill 1678, and other computer crime legislation.

As all of you probably already know, the Congress passed computer crime legislation last year as part of the Comprehensive Crime Control Act. Because of the press of legislative business, that computer crime measure did not receive thorough consideration by the Senate. It is also generally agreed that the statute that was enacted was not complete.

It is the purpose of this hearing, therefore, to consider the changes and additions that the present law requires.

In the area of computer crime, Congress has enjoyed the leadership of several individuals—Bill Hughes, Bill McCollum, Bill Nelson on the House side, Senator Mathias, Senator Cohen, and last, but certainly not least, Senator Paul Trible here in the Senate.

We are pleased to have you here with us, Senator Trible, to have the benefit of your assessment of the problems and the proposals for addressing the problems.

However, before turning to Senator Trible and the other distinguished witnesses who are present here today, I would like to outline briefly in behalf of the subcommittee the principal concerns that we have regarding Federal computer crime legislation and to mention some of the issues that I hope will be addressed by the witnesses.

BEST COPY AVAILABLE

It may be helpful to approach the problem as the ABA task force on computer crime recently did, by dividing the crimes into those in which certain computers or computer systems are the objects of criminal activity and those in which computers are used in the commission of other crimes. The principal problem that then confronts us is the determination of which of these crimes should be Federal crimes and which should be left to State and local authorities.

Speaking generally, it seems to me that Congress is justified in making it a Federal crime to gain unauthorized access to, or to damage or destroy, computers and computer software and data that are owned or operated by the Federal Government or by federally insured financial institutions. That, to this chairman, represents clear Federal jurisdiction.

The unauthorized obtaining of information contained in such computers should also be a Federal crime. On the other hand, it seems equally appropriate to leave to the States the same crimes of trespass, malicious mischief, and theft where the computers are privately owned and where there is no Federal interest in them or in the information they contain.

Between these two poles, there are crimes committed with computers owned by the Federal Government and by federally insured financial institutions, crimes involving exclusively private computers that contain information with a significant Federal interest, such as information protected by the Fair Credit Reporting Act, and crimes involving private computers that cannot practically be investigated and prosecuted by State and local authorities even though there is no clear Federal interest in either the computers or the data. So I would be particularly interested in any guidance that those of you who are going to testify today can offer the subcommittee in these latter areas.

We must also take into account the fact that computer technology, and with it, computer crime, is a rapidly changing field, I think probably as rapidly changing as this subcommittee or the full committee, for that matter, confronts today. We must do what we can to make sure that the criminal statutes keep up with those changes.

More than 35 States, I am informed, presently have computer crime statutes, and more will soon follow suit. Thus it is not only Congress, but the several States as well that are struggling with the problems posed by computer crime, and it behooves us here as elsewhere to learn what we can from their experience.

Given the difficulty of passing legislation and the even greater difficulty of making later changes or adjustments in Federal statutes, which is a monumental feat around here most of the time, it seems to me that the best course to follow is one of restraint, extending Federal jurisdiction where it is clearly appropriate—not otherwise—but deferring to States where it is not. That is a clean division which may or may not be practical. We will see as the testimony proceeds.

First I wish to place copies of S. 440 and S. 1678 in the record.

[Texts of S. 440 and S. 1678 follow:]

BEST COPY AVAILABLE

II

99TH CONGRESS
1ST SESSION

S. 440

To amend title 18, United States Code, to create an offense for the use, for fraudulent or other illegal purposes, of any computer owned or operated by certain financial institutions and entities affecting interstate commerce.

IN THE SENATE OF THE UNITED STATES

FEBRUARY 7 (legislative day, JANUARY 21), 1985

Mr. TRIBLE introduced the following bill; which was read twice and referred to the Committee on the Judiciary

---

A BILL

To amend title 18, United States Code, to create an offense for the use, for fraudulent or other illegal purposes, of any computer owned or operated by certain financial institutions and entities affecting interstate commerce.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That this Act may be cited as the "Computer Systems Protection Act of 1985".

SEC. 2. The Congress finds that—

(1) computer-related crime poses a serious threat to the Nation's economy;

BEST COPY AVAILABLE

(2) computer crimes tend to cause far higher losses than other white-collar crimes, and therefore create a heavy financial burden on the public;

(3) the Nation's growing reliance on high technology creates an opportunity for widespread computer abuse;

(4) computer-related crime directed at computers which operate in or use a facility of interstate commerce has a direct effect on interstate commerce;

(5) prosecution of persons engaged in certain computer-related crime is difficult under current Federal law; and

(6) the lack of effective prosecution often leads affected businesses to conceal computer crimes, and that no effective deterrent to such crimes exists as a result.

SEC. 3. Section 1030 of title 18, United States Code, is amended by—

(1) redesignating subsection (e) as subsection (f); and

(2) adding after subsection (d) the following new subsection:

"(e)(1) Whoever knowingly—

"(A) accesses a computer described in paragraph (4) without authorization, or

BEST COPY AVAILABLE

"(B) having accessed such a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend,

and thereby knowingly—

"(i) executes or attempts to execute a scheme or artifice to defraud;

"(ii) obtains or attempts to obtain the property of another;

"(iii) causes or attempts to cause the withholding or denial of the use of such computer; or

"(iv) modifies, damages, or destroys property of another,

shall be fined not more than two times the amount of the gain directly or indirectly derived from the offense or $50,000, whichever is higher, or imprisoned for not more than five years, or both.

"(2) Whoever knowingly and without authorization accesses a computer described in paragraph (4) shall be fined not more than $5,000 or imprisoned for not more than one year, or both.

"(3) This subsection does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a

BEST COPY AVAILABLE

political subdivision of a State, or an intelligence agency of the United States.

"(4) For purposes of this subsection, there is Federal jurisdiction over an offense if the computer—

"(A) is owned by, under contract to, or operated for or on behalf of a financial institution, and the prohibited conduct directly involves or affects the computer operation for or on behalf of the financial institution; or

"(B) operates in, or uses a facility of, interstate or foreign commerce.

"(5) For the purposes of this subsection, the term—

"(A) 'financial institution' means—

"(i) a bank with deposits insured by the Federal Deposit Insurance Corporation;

"(ii) the Federal Reserve or a member of the Federal Reserve including any Federal Reserve bank;

"(iii) a credit union with accounts insured by the Federal Savings and Loan Corporation;

"(iv) a credit union with accounts insured by the National Credit Union Administration;

"(v) a member of the Federal home loan bank system and any home loan bank;

BEST COPY AVAILABLE

"(vi) a member or business insured by the Securities Investor Protection Corporation; or

"(vii) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities and Exchange Act of 1934;

"(B) 'property' means anything of value, and includes tangible and intangible personal property; information in the form of computer processed, produced, or stored data; information configured for use in a computer; information in a computer medium; information being processed, transmitted, or stored; computer operating or applications programs; or computer services;

"(C) 'computer services' includes computer data processing and storage functions;

"(D) 'computer medium' includes the means of effecting or conveying data for processing in a computer, of a substance or surrounding medium which is the means of transmission of a force or effect that represents data for processing in a computer, or a channel of communication of data for processing in a computer; and

"(E) 'computer program' means an instruction or statement or a series of instructions or statements in a form acceptable to a computer, which permits the func-

BEST COPY AVAILABLE

tioning of a computer system in a manner designed to provide appropriate products from such computer system.

"(6)(A) Notwithstanding subsection (d), in a case in which Federal jurisdiction over an offense as described in this subsection exists concurrently with State or local jurisdiction, the existence of Federal jurisdiction does not, in itself, require the exercise of Federal jurisdiction, nor does the initial exercise of Federal jurisdiction preclude its discontinuation.

"(B) In a case in which Federal jurisdiction over an offense as described in this subsection exists or may exist concurrently with State or local jurisdiction, Federal law enforcement officers, in determining whether to exercise jurisdiction, shall consider—

"(i) the relative gravity of the Federal offense and the State or local offense;

"(ii) the relative interest in Federal investigation or prosecution;

"(iii) the resources available to the Federal authorities and the State or local authorities;

"(iv) the traditional role of the Federal authorities and the State or local authorities with respect to the offense;

"(v) the interests of federalism; and

"(vi) any other relevant factor.

BEST COPY AVAILABLE

"(C) The Attorney General shall—

"(i) consult periodically with representatives of State and local governments concerning the exercise of jurisdiction in cases in which Federal jurisdiction as described in this subsection exists or may exist concurrently with State or local jurisdiction;

"(ii) provide general direction to Federal law enforcement officers concerning the appropriate exercise of such Federal jurisdiction which, for the purposes of investigation, is vested concurrently in the Department of Justice and the Department of the Treasury;

"(iii) report annually to Congress concerning the extent of the exercise of such Federal jurisdiction during the preceding fiscal year; and

"(iv) report to Congress, within one year of the date of enactment of this subsection, on the long-term impact of this subsection upon Federal jurisdiction and the increasingly pervasive and widespread use of computers in the United States (the Attorney General shall periodically review and update such report).

"(D) Except as otherwise prohibited by law, information or material obtained pursuant to the exercise of Federal jurisdiction under this subsection may be made available to State or local law enforcement officers having concurrent jurisdiction, and to State or local authorities otherwise assigned re-

BEST COPY AVAILABLE

sponsibility with regard to the conduct constituting the offense.

"(E) An issue relating to the propriety of the exercise of or of the failure to exercise Federal jurisdiction over an offense as described in this subsection, or otherwise relating to the compliance, or to the failure to comply, with this subsection, may not be litigated, and a court may not entertain or resolve such an issue except as may be necessary in the course of granting leave to file a dismissal of an indictment, an information, or a complaint.".

○

BEST COPY AVAILABLE

II

99TH CONGRESS
1ST SESSION

S. 1678

To amend title 18, United States Code, to protect the use of Federal computer systems against fraud and abuse.

IN THE SENATE OF THE UNITED STATES

SEPTEMBER 20 (legislative day, SEPTEMBER 16), 1985

Mr. THURMOND (for himself, Mr. BIDEN, Mr. EAST, Mr. HATCH, Mr. LAXALT, and Mr. MCCONNELL) (by request) introduced the following bill; which was read twice and referred to the Committee on the Judiciary

---

A BILL

To amend title 18, United States Code, to protect the use of Federal computer systems against fraud and abuse.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That this Act may be cited as the "Federal Computer Systems Protection Act of 1985".

SEC. 2. (a) Section 1030 of title 18, United States Code, is amended to read as follows:

"§ 1030. Computer fraud and abuse

"(a) Whoever having devised or intending to devise any scheme or artifice to defraud or for obtaining money or property by false or fraudulent pretenses, representations, or

BEST COPY AVAILABLE

promises, or to embezzle, steal, or convert to his use or the use of another, property not his own, for the purpose of executing such scheme or artifice or embezzlement, theft or conversion or attempting to do so, knowingly obtains access to or attempts to obtain access to a computer shall—

"(1) if the computer is owned by, under contract to, or operated for or on behalf of—

"(A) the United States Government; or

"(B) a financial institution; or

"(2) if in committing or concealing the offense of two or more computers are used which are located in different States or in a State and a foreign country,

be fined not more than $250,000, or imprisoned not more than five years, or both.

"(b) Whoever knowingly and willfully without authorization damages, destroys, or attempts to damage or destroy a computer described in subsection (a)(1) or any computer program or data contained in such computer shall be fined not more than $250,000 or imprisoned not more than five years, or both.

"(c) Whoever intentionally without any authorization obtains access to a computer described in subsection (a)(1) or a computer system or computer network including such computer, shall be guilty of a misdemeanor and shall be fined not

BEST COPY AVAILABLE

more than $100,000 or imprisoned not more than one year, or both.

"(d) Whoever violates any provision of subsection (a), (b), or (c) shall forfeit to the United States any interest acquired or maintained in any computer and computer program, which has been used to commit the violation. Upon conviction under this section the court shall authorize the Attorney General to seize all property or other interest declared forfeited under this section upon such terms and conditions as the court shall deem proper. If a property right or other interest is not exercisable or transferable for value by the United States, it shall expire, and shall not revert to the convicted violator. The United States shall dispose of all such property as soon as commercially feasible, making due provision for the rights of innocent persons.

"(e) The Attorney General is authorized to delegate, in whole or in part, to other departments and agencies concurrent investigative authority under this section subject to agreement between the Attorney General and the department or agency affected.

"(f) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.

BEST COPY AVAILABLE

58-745 O - 86 - 2

"(g) For the purposes of this section—

"(1) the term 'computer' means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions and includes any data storage facility or communications facility directly related to or operating in conjunction with such device;

"(2) the term 'computer system' means a set of related connected or unconnected computers, computer equipment, devises, and software;

"(3) the term 'computer network' means two or more interconnected computers, computer terminals, or computer systems;

"(4) the term 'computer program' means an instruction or statement or a series of instructions or statements, in a form that is designed to permit the functioning of a computer system;

"(5) the term 'computer services' includes computer operating time, data processing, and data storage;

"(6) the term 'financial institution' means—

"(A) a bank with deposits insured by the Federal Deposit Insurance Corporation;

"(B) the Federal Reserve or a member of the Federal Reserve Bank;

BEST COPY AVAILABLE

"(C) an institution with accounts insured by the Federal Savings and Loan Corporation;

"(D) a credit union with accounts insured by the National Credit Union Administration;

"(E) a member of the Federal Home Loan Bank system and any home loan bank;

"(F) a member or business insured by the Securities Investor Protection Corporation; and

"(G) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities and Exchange Act of 1934;

"(7) the term 'financial instrument' means any check, draft money order, certificate of deposit, letter of credit, bill of exchange, credit card, debit card, or marketable security;

"(8) the term 'obtains access' means to communicate with, in order to instruct, store data in, retrieve data from, or otherwise make use of any resources of a computer, computer system, or computer network;

"(9) the term 'property' includes financial instruments, information, including electronically processed or produced data and computer programs in either machine or human readable form; computer services; and any other tangible or intangible item of value; and

BEST COPY AVAILABLE

"(10) the term 'United States Government' includes a branch or agency thereof.".

(b) The item relating to section 1030 in the table of sections of chapter 47 of title 18, United States Code, is amended to read as follows:

"1030. Computer fraud and abuse.".

O

Senator LAXALT. So, with these very general comments in mind, I am very happy to turn first to my friend and distinguished colleague from the great State of Virginia, Paul Trible.

STATEMENT OF HON. PAUL S. TRIBLE, JR., A U.S. SENATOR FROM THE STATE OF VIRGINIA

Senator TRIBLE. Mr. Chairman, I thank you for the warmth of your welcome and your very kind words, and I want to express my appreciation for your convening today's hearing.

It is a pleasure to be here and to have the opportunity to address a real and growing danger—computer crime.

During the 98th Congress and again this year, I have sponsored legislation that would impose tough new penalties on computer criminals. Last year, the Congress took an important and overdue step by inacting the first Federal Computer Crime Statute. That law afforded a measure of protection to computer data relating to national security and to individuals' credit histories.

But today, there remains a vast array of computerized data that is wholly unprotected against acts of theft, vandalism, and trespass In the Government's race to protect this computer data against crime, the hour is late. Quite simply, the criminals have the technological edge.

One of Virginia's major newspapers, the Richmond Times-Dispatch, recently reported several new and disturbing examples of computer activity in the criminal area. They described several computer bulletin boards whose principal purpose was to assist people in breaking into computer systems operated by the Defense Department, the Walter Reed Medical Center, and the Republican National Committee.

Senator LAXALT. I could tolerate DOD, but the Republican National Committee is something else.

Senator TRIBLE. That is right. I knew that would get your attention, Mr. Chairman.

Moreover, computer crime appears to afflict the vast majority of Government and private sector computer users. A recent American Bar Association survey found that almost one-half of those compa-

BEST COPY AVAILABLE

nies and Government agencies that responded had been victimized by some form of computer crime. The known financial loss from such crimes was estimated as high as $730 million.

A general consensus emerged from that survey on the danger of computer crime and how best to attack it. According to the ABA report, computer crime is among the worst white-collar crimes facing our Nation. It is a defense that demands new and heavy criminal penalties. Fully 80 percent of those questioned by the ABA support enactment of a Federal computer crime statute.

So today, we need to explore and refine exactly what form a new Federal computer crime statute should take.

As you know, Mr. Chairman, I am the sponsor of Senate bill 440, the Computer Systems Protection Act. This bill was designed to supplement the law passed last year by extending Federal jurisdiction to banking institutions and to private companies whose computers operate in interstate commerce.

With your cooperation and assistance, I have been revising Senate bill 440 to narrow the scope of Federal jurisdiction while ensuring that a broader range of criminal conduct is covered, including acts of simple trespass and destruction of property. It is my hope, building on today's hearing, that we can introduced a revised computer crime bill that will form the basis of prompt congressional action.

Let me briefly discuss the principles that I hope to see embodied in a new Federal computer crime statute.

First and foremost, I believe the 99th Congress should supplement, rather than supplant, the computer crime statute enacted by Congress last year. That statute laid a good foundation on which we can build.

Second, we must ensure that computers of the Federal Government and of the Nation's banking system are protected against all forms of malicious mischief. Intentional damage or destruction of computerized property must be punished as surely as we now punish abuses of more traditional forms of property.

In addition, we must protect computerized data belonging to the Government or the Nation's banks against modification or denial of access. For example, it should be a crime for anyone acting with a malicious intent to alter the numbers contained in a banks accounting system, or to change the bank's computer code so that it can no longer access its own computer data.

We in the Congress must also protect Government and bank computers against simple acts of trespass. Frequently, an offender who has accessed a computer without authorization will not steal or damage the computer data. Nevertheless, the offender is treading where he ought not be, and he should be punished just as surely as someone who walks onto sensitive Government property without proper authorization can be prosecuted by the Federal authorities.

Finally, we must examine closely the degree to which the same protections should be afforded to private companies engaging in interstate commerce. In those cases where interstate acts of computer theft, abuse and trespass cannot be addressed by State and local prosecutors, it is essential that Congress take action. Today we will hear from local prosecutors who can sketch more complete-

BEST COPY AVAILABLE

ly the problems they face at the State level in responding to this new menace.

In summary, I believe a new computer crime bill should stem the use of our Nation's new technologies as tools of crime, protect the vast amounts of commerce that now take place via computer, and dispel the mistaken notion that computer crime is merely a game, or a challenge to be overcome.

I look forward to working with you, Mr. Chairman, and with the Justice Department and others to fashion and pass such legislation.

[The following was subsequently supplied for the record:]

BEST COPY AVAILABLE

Associated Credit Bureaus, Inc.

November 6, 1985

The Honorable Paul Laxalt
Chairman
Subcommittee on Criminal Law
Senate Committee on Judiciary
323A Senate Russell Office Building
Washington, D.C. 20510

Dear Chairman Laxalt:

Per the request of Senator Trible's office, we are submitting the attached statement for the record as the Subcommittee deliberates S. 440, S. 1678 and other computer crime legislation.

We appreciate your desire to have a complete record on this most important issue and the opportunity to submit this statement for the record.

Very truly yours,

Steven I. Fier
Director of Government Relations
and Legislative Counsel

Attachment

Government Relations Office
1350 New York Avenue, N.W., Suite 1025 • Washington, D.C. 20005 • (202) 628-8090

BEST COPY AVAILABLE

Associated Credit Bureaus, Inc.

STATEMENT OF WALTER R. KURTH

PRESIDENT OF ASSOCIATED CREDIT BUREAUS, INC.

ON

S. 440 "The Computer Systems Protection Act";

S. 1678 "The Federal Computer Systems Protection Act of 1985";

and Other Computer Crime Legislation

Before the Subcommittee on Criminal Law

of the

Senate Committee on The Judiciary

United States Senate

Washington, D.C.

October 30, 1985

Government Relations Office
1350 New York Avenue, N.W., Suite 1025 • Washington, D.C. 20005 • (202) 628-8060

BEST COPY AVAILABLE.

On behalf of the 1,400 members of Associated Credit Bureaus, Inc. (ACB), an international trade association founded in 1906 to represent the consumer credit reporting industry, we are pleased to submit for the record the following statement to the Senate Judiciary Subcommittee on Criminal Law as it deliberates S. 440, S. 1678 and other computer crime legislation. While computer security remains a primary and integral part of the management effort of automated credit bureaus, computer vulnerabilities, both real and imagined, provide the basis for ongoing Congressional efforts to protect information resources.

Before proceeding with our comments, we would first like to applaud the actions of the Chairman whose efforts last year resulted in the inclusion of the Federal computer crime language in Public Law 98-473.

Last year, with ACB's support, Congress enacted legislation specifically making it a federal offense to access a consumer credit bureau computer without authorization. Specifically, Section 1030 (a) (2) of the Comprehensive Crime Control Act of 1984 (Public Law 98-473) states:

> "whoever knowingly accesses a computer without authorization, or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend, and thereby obtains information...contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C.1681 et seq.)" shall be subject to the following maximum penalties:

First offense: a fine of $5000 or twice the value or loss created by the offense, and imprisonment for one (1) year;

Second offense: a fine of $10,000 or twice the value obtained or loss created by the offense, and imprisonment for ten (10) years.

BEST COPY AVAILABLE

For the reasons discussed below, we believe that the legislation enacted last year has made great strides towards preserving the integrity of consumers' credit histories, and therefore, we strongly oppose the provisions in S. 1678 which would repeal existing Section 1030 (a)(2) and replace it with more general language.

- The Fair Credit Reporting Act was enacted by Congress in recognition of the interstate nature of the industry to restrict the dissemination of information contained in a file maintained by a consumer reporting bureau relating to an individual's credit history. Existing Section 1030 has provided the credit bureau industry with an excellent tool to further enhance Congressional intent in enacting the Fair Credit Reporting Act. Therefore, to repeal Section 1030 would be taking a major step backward.

- ACB supports Congressional efforts to safeguard other types of equally sensitive and confidential information. However, Congress should not repeal the protection it has provided credit bureaus and consumers because it has not enacted legislation to protect other types of confidential information.

- The law is working, it is providing credit bureau management with an effective tool to be used in the hiring of credit bureau personnel and the selling of information within the intent of the Fair Credit Reporting Act.

- The credit reporting industry protections in the law are equally as important to credit granters, banks, retailers etc. because a primary reason to tamper with a credit bureau computer is to access records in order to obtain credit information and subsequently defraud credit granters.

- S. 1678 instead of tightening the law would create loopholes enabling criminals "hacking" credit bureau files to escape prosecution.

While ACB remains firm in its support for the retention of the provisions in existing Section 1030 providing protection to computers

BEST COPY AVAILABLE

owned and operated by consumer reporting agencies, it is also our view that the stiffer criminal penalties contemplated in S. 440, S. 1677 and S. 1678 will go a long way in further deterring "hackers" from committing computer crimes.

As the Subcommittee knows, there has been a tendency on the part of the public to view computer crime as a form of intellectual pranksterism. Because of this inaccurate perception, societal definitions, deterrents and punishments are needed to control these white-collar crimes. The enactment of stronger criminal penalties will send a clear signal to those perpetrating computer crimes that there is as much wrongdoing in taking or abusing information contained in computers as there is in mugging a little old lady and taking her pocketbook. Therefore, ACB supports the strengthened criminal penalty provisions of S. 440, S. 1667 and S. 1678 as potential legislative vehicles for the further deterrence of computer crimes. However, we strongly believe that any federal computer crime legislation passed by the Congress must continue to make it a crime to illegally access a consumer reporting agency computer.

Crime has moved into the computer age and we support Congressional efforts to respond accordingly. ACB wishes to express its appreciation to the Subcommittee for the opportunity to submit this statement for the record and would be pleased to respond to any questions the Subcommittee may have.

BEST COPY AVAILABLE

Senator LAXALT. I thank the Senator for an excellent statement, and as your time and schedule permit, I certainly welcome you to the rostrum here to assist me in the conduct of these hearings.

Senator TRIBLE. I would like to join you.

Thank you, Mr. Chairman.

Senator LAXALT. Thank you. The record should note the presence of the distinguished chairman of the full committee.

Senator Thurmond, welcome. Senator Thurmond, we have just concluded the opening statement of Senator Trible, as you know, one of the principal sponsors of the new legislation.

Is it your wish to have an opening statement of any sort?

The CHAIRMAN. Yes; I have a brief statement, Mr. Chairman, if I may.

Senator LAXALT. We would be delighted to hear it, Mr. Chairman.

OPENING STATEMENT OF CHAIRMAN STROM THURMOND

The CHAIRMAN. Mr. Chairman, today the Criminal Law Subcommittee of the Senate Committee on the Judiciary will be examining S. 440, the Computer Systems Protection Act of 1985, S. 1678, the Federal Computer Systems Protection Act of 1985, and other legislative initiatives in the evolving area of computer fraud.

The expanding technologies and growing use of computers in the commission of crimes have heightened the need for more effective legislation. As a result of hearings in the House of Representatives, new language addressing computer crime was added to the Comprehensive Crime Control Act when the bill was in conference during the last Congress. My good friend, Senator Paul Laxalt, the able chairman of this subcommittee, is to be commended for his assistance on that comprehensive anticrime initiative and for holding this important hearing today.

As many of you are aware, in September, the administration announced an eight-point package of antifraud legislation. Among its provisions was an initiative specifically designed to enhance our ability to prosecute those who engage in computer-related crimes.

On September 20, on behalf of the administration, I introduced to S. 1678, the Federal Computer Systems Protection Act of 1985. That bill, along with the other parts of the antifraud initiative, will reform and reinforce Government efforts to prevent waste, fraud, and abuse in Federal programs.

As I stated when I introduced the antifraud package, it is time that those who defraud the Government are put on notice that these fraudulent and illegal practices will be met with swift and aggressive prosecution.

We have an impressive list of witnesses prepared to discuss the computer fraud bills before this subcommittee. I would like to welcome them. I would also like to join with the members of the subcommittee in welcoming our distinguished and able colleague, Senator Trible of Virginia, who has introduced S. 440, and who has been a leader in our attempt to keep pace with the rapid developments in the area of computer fraud.

As a member of this subcommittee and chairman of the full committee, I look forward to working with other members of this subcommittee, Senator Trible, and the administration to develop the most effective legislation possible in this area.

BEST COPY AVAILABLE

I have another conflict this morning and will not be able to remain, but again, Mr. Chairman, I want to commend you for your leadership in this matter.

Senator LAXALT. I thank the chairman. I do not know of any busier Senator in this whole place than Senator Strom Thurmond, so your absence to another commitment is readily understood.

We thank you for your help, Mr. Chairman.

The CHAIRMAN. Thank you.

Senator LAXALT. Very well. We will proceed now with our various witnesses, and we will commence with Victoria Toensing, the Deputy Assistant Attorney General, Criminal Division, Department of Justice.

Welcome, Ms. Toensing. We are delighted to have you here.

STATEMENT OF VICTORIA TOENSING, DEPUTY ASSISTANT ATTORNEY GENERAL, CRIMINAL DIVISION, DEPARTMENT OF JUSTICE

Ms. TOENSING. Good morning, Mr. Chairman and Senator Trible.

Thank you for asking me here to speak about the computer crime legislation. Each of our branches has been concerned about the vast potential for criminal abuse of computers. Last year, as you stated earlier, Mr. Chairman, a new section was passed now called 18 U.S.C. 1030 which proscribes certain computer-type offenses. We all agree, however, that 1030 is inadequate for most computer crimes and that we must address anew this area for criminality.

Let me briefly describe 1030's limited coverage so we can see where the gaps are and the need for additional legislation. In general, 1030 prohibits unauthorized computer access in three basic situations. First is the genre of classified information where it is listed in 1030. Unauthorized access to the kinds of classified information set forth in 1030 is a felony.

While the Justice Department agrees this conduct should be criminal, it is indeed already so under certain espionage statutes.

Furthermore, 1030 would rarely be used by the prosecutor, because the espionage statutes have a lower scienter requirement. One only has to prove that the defendant had "a reason to believe that that information could be used" to harm the United States, or to the advantage of a foreign country. In contrast, 1030 requires that the defendent knew that the information "is to be used"—a much higher standard. So you see, it is not a very good tool for the prosecutor, who would probably not ever want to use that.

Senator LAXALT. Is 1030, other than the burden situation, more comprehensive in coverage?

Ms. TOENSING. I do not believe so. [Conferring with staff.]

Senator LAXALT. It is not?

Ms. TOENSING. No; my experts agree.

The second area addressed by 1030 is that of protecting consumer-type records. Under 1030, only certain records of mostly individuals or partnerships of under five people are protected from unauthorized access. The first offense would be a misdemeanor, and then after that it is a felony.

BEST COPY AVAILABLE

This provision offers very limited protection and then, only to very specific kinds of financial or credit-type information. If the rationale behind the statute is to protect personal records, then why not tax return records or census data records. Moreover, what about the small business that happens to be incorporated? Under 1030 the incorporated small business is not protected. In addition, while I understand large corporations are not in vogue at this time, the information generated by a large corporation that might be trying to secure a line of credit, for example, should be protected because the corporation's stockholders and employees could be affected by publication of financial information.

Senator LAXALT. Your point being the present statute does not cover that kind of activity?

Ms. TOENSING. That is correct, Mr. Chairman; only individuals or partnerships of five and less persons.

Senator LAXALT. So you would extend this, then, to corporations. What other extension?

Ms. TOENSING. If our rationale is that we should be protecting financial information, then it should be protected across-the-board.

Senator LAXALT. In terms of entities.

Ms. TOENSING. That is correct. It is sort of a vertical kind of concept there.

Senator LAXALT. Do you know at all what the rationale was for the limitation in the present bill? Was it just a matter of simplicity?

Ms. TOENSING. I do not know.

Senator LAXALT. There is no way you would know.

Ms. TOENSING. It was in the House.

Senator LAXALT. So, who knows—who knows the wanderings of the congressional mind.

Senator TRIBLE. Especially in the House of Representatives.

Senator LAXALT. Well, you can say that; I cannot.

Ms. TOENSING. I might say that every time I testify in the other body about something that got passed in the crime bill, they say, "Well, we do not know a whole lot about this, because we did not have a chance to have a hearing on it." For the first time I have heard that about something in the Senate.

Senator LAXALT. I think that is a lot of the problem, really; it was thrown together in a hurry.

Ms. TOENSING. Not the bill that came out of the Senate, though, Mr. Chairman. That was very well thought out.

Senator LAXALT. No; I like to think it had rather thorough consideration, as is always the case.

Ms. TOENSING. The third kind of—it is really a situation more than a type of information—that we have under 1030, is destruction or disclosure of information if the access was not authorized. That is (a)(3) under 1030. This provision is violated, however, only if the computer is operated on behalf of the U.S. Government, and then, only if—that does not bother me, but the next sentence does. I call them federally operated computers for shorthand. But only if such conduct affects such operation. I used to be an English teacher before I went to law school, and that would mean grammatically—if it affects the operation of the computer. But the legislative history, as I understand it, means if it affects the operation of the

BEST COPY AVAILABLE

Government. I am not sure what any of us could walk into court with on that. More precisely, I am not sure how many people can actually affect the operation of the Government. Consequently, that qualifying language presents a problem, and a very big problem.

So there we have it. Our present law is very limited in coverage, and it is not very useful to the prosecutor.

Senator LAXALT. Has that been your practical experience in Justice? What kind of experience have we had in Justice thus far under the existing statute? Have you had many prosecutions—just ballpark? Has there been extended activity, or are you just now getting into—one of your staff aides is raising four fingers. That indicates you have had four prosecutions?

Ms. TOENSING. Yes; I have found the piece of paper if you want the information. I can provide you with this.

Senator LAXALT. No; that is all right. I just wanted to get a general feel of what kind of activity had been under the existing statute and what that experience has been. Apparently, it has been rather limited. All right.

Ms. TOENSING. Yes; access to Government Treasury checks, credit cards things like that.

I would like to go over where we would like to go in the legislation. We really have four main points to make. The first is that we agree that unauthorized access to a Federal computer should be prohibited. But we do not see any reason for a requirement that this information be obtained or that it prevented someone else from legitimately accessing the computer.

First of all, we are not quite sure what obtained means. Remember the movie "War Games," where the kid changed the "C" to an "A"? Well, he probably did not, obtain, that under a legal standard that the courts would start to hand down.

We do not have a legal standard for obtain, and I am afraid that this kind of word would dictate a more exacting standard changing or using. We would prefer to see changing or using in there because this kind of language would produce a lesser standard.

Federal computers, we feel, should be protected, period. That is it. The people who do not have access to the information should not be in there, for whatever purpose. We have a clear Federal interest in protecting the information in either Federal computers or computers that are operated by Federal financial institutions such as banks and savings and loans.

Our second main point is that we think that there should be a fraud offense specifically covering computers. The present fraud statutes were written prior to computers coming into frequent use. Under existing laws we may not be able to make the technical adjustment over to the computer area.

We view the computer as a vehicle through which the fraud is committed. Accordingly, a computer is not mail and it is not wire. The computer is the vehicle, and we are going to have to have something that covers it as the vehicle.

Senator LAXALT. You are satisfied, then, that the existing fraud statutes would not adequately cover the prosecution of a computer-related fraud crime—or at least you are uncertain, and you would want that reinforced. Is that your point?

BEST COPY AVAILABLE

Ms. TOENSING. Yes; that is correct, Mr. Chairman.

Senator LAXALT. OK.

Ms. TOENSING. In a few cases, we have managed to obtain guilty pleas, because we have had a situation where in one case, although the thrust was using a computer, the person used the mail for something. As a result, we were able to put together a mail fraud case. But I am quite certain that sooner or later, we are going to run into some factual situations where we cannot slip the step-sister's foot into Cinderella's slipper, and we will need a statute that really covers computer fraud.

Our legislation proposes a fraud offense to attach in three separate situations: If it is a Federal computer, if it is a Federal financial institution, or if the computer is located in two or more States, or in one State and in a foreign country.

I would like to address your concern, Mr. Chairman, that we only should be going where Federal jurisdiction is needed. You could not find an Attorney General or the policy of a Justice Department more in agreement with you. I think you are aware of that. There is a very big concern that we should not be there when the States can be there. When a fraud crosses State lines, however, States cannot be there. If a fraud were committed that went from one State to another, uniquely, it is a Federal kind of jurisdiction. That is why we want this kind of jurisdiction.

We also would like to point out that we oppose a provision that was passed in the House last year that required the Government to prove that the defendant was not authorized to have access in a fraud case. We feel if somebody has access and they commit a fraud; that is, if the information is diverted illegally, they should not get a free ride just because they had authorized access to the computer. The evil was that they committed the fraud, not whether their access to the information needed to commit their crime was authorized or unauthorized.

Our last point, Mr. Chairman, is that we recommend a criminal forfeiture provision where the defendant's interest in the computer involved in the crime could be forfeited to the Government up on conviction. It would only be after conviction that we would have the forfeiture, but we think that this is an appropriate kind of a sentence, because we have found historically that judges are rather reluctant to sentence someone who is committing a crime with a computer. There is a certain hesitancy to send these kinds of people to jail. We must have some kind of sanction to prevent this kind of crime. Quite possibly, taking away this person's most beloved object, the hacker's computer, is the best way to do it.

That is all I have, Mr. Chairman. I have a more complete statement for the record, and I would ask that that be submitted.

Senator LAXALT. I thank you, and it will be filed.

[Statement follows:]

BEST COPY AVAILABLE

PREPARED STATEMENT OF VICTORIA TOENSING, DEPUTY ASSISTANT ATTORNEY GENERAL, CRIMINAL DIVISION, DEPARTMENT OF JUSTICE

Mr. Chairman and Members of the Subcommittee, I am pleased to be here today to present the views of the Department of Justice on Computer Crime legislation. The potential for the use of computers in a variety of criminal schemes has been well documented. The Congress dealt with this sometimes complex subject in the Comprehensive Crime Control Act of 1984 and the result is a new section of the criminal code, 18 U.S.C. 1030, which proscribes certain computer related offenses.

Nevertheless, section 1030 in its present form is inadequate and revisions must be made for a really effective federal computer crime statute. In this regard, the Administration has prepared a computer crime bill, S. 1678, that would substantially improve the federal computer crime statute. This proposal is part of the President's comprehensive management reform legislation initiative, which he announced on July 31, 1985. Let me first outline the existing provisions in section 1030 and describe some of their shortcomings. Then I will explain why the concepts contained in the Administration's computer crime proposal merit serious and favorable consideration.

18 U.S.C. 1030 sets out three distinct computer-related offenses. Subsection 1030(a)(1) proscribes the use of a computer without authority or in excess of one's authority to obtain classified information or restricted data relating to national defense, foreign relations, or the Atomic Energy Act of 1954. Clearly, the unauthorized obtaining of this type of data is a serious matter and deserves to be punished as a felony. That much of these data are stored in computers has made them much more

BEST COPY AVAILABLE

vulnerable to unauthorized disclosure than they were a generation ago. Nevertheless, the offense in subsection (a)(1) is largely redundant and unnecessary, because other statutes proscribe the unauthorized possession or retention of the same information and provide for the same or harsher penalties, regardless of whether or not a computer is used. 1/ In short, subsection 1030(a)(1), while not harmful, is simply not very helpful to federal prosecutors. It is quite hard to imagine a case in which it would be easier to use this provision in prosecuting a criminal case than one of the older offenses that prohibit unauthorized access to important national security information.

Subsection 1030(a)(2) proscribes using a computer without authority or in excess of one's authority to obtain information contained in a "financial record" of a "financial institution," as those terms are defined in the Right to Financial Privacy Act of 1978, 2/ or to obtain information in a file of a "consumer reporting agency" on a "consumer," as those terms are defined in the Fair Credit Reporting Act. 3/ This offense is a misdemeanor, although a second conviction under this subsection would be treated as a felony. We certainly agree that this type of extremely revealing information about a person's financial affairs should not be disclosed without authorization. The fact

---

1/ 18 U.S.C. 793, 794; 42 U.S.C. 2275; 50 U.S.C. 783.

2/ 12 U.S.C. 3401 et seq.

3/ 15 U.S.C. 1681 et seq.

BEST COPY AVAILABLE

that a lot of it is stored in computers has undoubtedly made it more vulnerable to such disclosure. For that reason, subsection 1030(a)(2) may be of some limited utility.

It is unjustifiable, however, to single out only a very limited class of financial and credit information for protection against unauthorized computer access. For example, 1030(a)(2) prohibits unauthorized access to a bank's computer to obtain information contained in the account of an individual or a partnership of five or fewer persons, but would give no protection to corporate accounts or to the bank's own records of its deposits in other institutions and loans because these are not within the purview of the Right to Financial Privacy Act. The subsection would, for similar reasons involving the scope of the Fair Credit Reporting Act, prohibit the unauthorized obtaining of credit information on an individual but not on even the smallest of corporations. Simply put, it makes no sense to restrict this offense to unauthorized computer access to personal financial records. If the objective of subsection (a)(2) is to protect against the use of computers to obtain certain personal information concerning individuals which enjoys, through operation of other federal laws, a high degree of confidentiality -- a laudable goal -- the use of computers to obtain many other types of personal information (such as tax return information and census data) should also be covered.

Subsection 1030(a)(3) proscribes using a computer without authority or in excess of one's authority, and by means of such conduct using, modifying, destroying, or disclosing information

BEST COPY AVAILABLE

in the computer or preventing authorized use of the computer "if such computer is operated for or on behalf of the Government of the United States and such conduct affects such operation." This offense also is a misdemeanor, but a second conviction would be punished as a felony. We certainly agree that unauthorized access to the computers of the federal government should be a crime. Subsection (a)(3) is inadequate because it is not a true unauthorized access offense. Instead, it requires the using, modifying, destroying or disclosing of the information or preventing authorized use of the computer. As I will explain in more detail shortly when I outline the Administration's bill, we think the unauthorized access offense, particularly with respect to the federal government's computers, is most like a physical trespass onto government property or into a government building and should be punishable without a showing that the person made any use of or destroyed any information, or that he or she prevented any other person from gaining access to the computer.

Moreover, as I indicated, subsection 1030(a)(3) contains a jurisdictional element that could limit its usefulness even further. The proscribed conduct is a federal crime only if the computer involved "is operated for or on behalf of the Government of the United States and such conduct affects such operation." Grammatically, it would seem that this should be read to require the government to prove that the person's conduct affected the operation of the computer. However, the legislative history of this provision indicates that the prosecutor must prove that the unauthorized access to and use or destruction of the information

BEST COPY AVAILABLE

in the computer affected the operation of the government. 4/ That will usually be a very difficult element to prove since unauthorized access to a government computer will likely have only a de minimis effect on even the agency involved. Even if it were clearly spelled out that such a trivial effect is all that is required, the presence of this element can only serve to divert the jury's attention from the crucial question at issue which is whether the defendant committed a trespassory type offense against government records and information. In our view, every such trespass should be considered a crime without proof of how seriously the intrusion affected the government.

At this point, Mr. Chairman, I think it would be helpful for me to set out some concepts that the Administration believes should be included in any revision of the computer crime provisions in section 1030. Each of the concepts is incorporated in our computer crime bill, S. 1678. First, as I have just discussed, it should be an offense to willfully obtain unauthorized access to a computer owned by or operated on behalf of the United States, without a showing that any information was obtained or that the unauthorized access prevented someone else from

---

4/ This provision was originally included in H.R. 5616 which passed the House on July 24, 1984. The parts of this bill that are now 18 U.S.C. 1030 were then included as a last minute amendment to the Comprehensive Crime Control Act, the legislative history of which makes no mention of the computer crime provision. For a brief discussion of the provision in H.R. 5616 which became 18 U.S.C. 1030(a)(3) see House Report No. 98-894, 98th Cong., 2d Sess., July 24, 1984, p. 22.

BEST COPY AVAILABLE

legitimately accessing the computer. Clearly, protecting the federal government's own computers is an altogether proper matter for federal jurisdiction. While we realize that many states now have computer crime provisions and that in theory these statutes could be applied to offenses against federal computers, it is not realistic to expect the states to take on this responsibility.

Unauthorized access to a computer owned by or operated on behalf of a federally insured financial institution should also be a federal offense. There is a very clear federal interest in protecting these institutions such as banks, savings and loans, and brokerage firms against computer crimes.

Second, we believe there should be a computer fraud offense. One of the most important reasons for having any federal computer offense is that computers may allow an old fashioned crime like theft or embezzlement to be committed in such a way that existing federal statutes do not cover it. As you know, federal jurisdiction over offenses of this type is grounded on such factors as the Commerce Clause, which justifies the federal mail and wire fraud statutes (18 U.S.C. 1341 and 1343) and federal regulation and insurance of many types of financial institutions which justifies such offenses as the new bank fraud statute (18 U.S.C. 1344), and the theft and embezzlement offense set out in 18 U.S.C. 656.

There is, however, a potential problem with the use of fraud or theft statutes, since these statutes antedate the invention and widespread use of computers. I stress that this is a

BEST COPY AVAILABLE

potential problem because so far at least we have been able to prosecute computer fraud cases under existing statutes. For example, in a case in which a person made telephone access approximately fifty times to the computer system of a previous employer to steal confidential software, two of the calls were made across state lines which brought into play the wire fraud statute. In another case, a former employee of the Federal Reserve Board gained access to information in the Board's file that kept track of money supply information that would have been very useful to clients in his new job as a private financial analyst. Fortunately, the defendant in that case eventually pled guilty to a violation of 18 U.S.C. 1001, in essence admitting that his making an unauthorized access to the Federal Reserve Board's computer constituted a "false statement." If he had not pleaded, proving a violation of 18 U.S.C. 1001 under these facts would have been difficult, and prosecuting the defendant for theft of government property would have been problematical because proving the value of the information about the money supply, a necessary element of proof, also would have been arduous.

In the future we may not be so fortunate. Consequently, there should be enacted a specific offense, as contained in our bill, modeled on the mail and wire fraud statutes, of devising a scheme or artifice to defraud, or to obtain money or property by false or fraudulent pretenses, or to embezzle, steal, or convert the property of another if, for the purpose of carrying out the offense the defendant accesses a computer with a particular federal nexus. The computer is thus the vehicle -- comparable to

BEST COPY AVAILABLE

the mails or interstate telephone wires -- through which the fraud offense is committed.

Under our proposal, federal jurisdiction would attach to the computer fraud offense in cases in which the computer involved is owned by or operated on behalf of the federal government or a federally insured financial institution, or if the offense involves computers located in two or more states or in a state and a foreign country. This two-state provision (which is far less of an assertion of federal jurisdiction than would be a provision to extend jurisdiction over a fraud scheme involving any computer operating in or affecting interstate commerce) would reserve federal jurisdiction for those cases where it is most needed and for those which the states are the least capable of investigating and prosecuting. For example, a state's laws only apply within its borders and it is unrealistic to expect a state to undertake the investigation and prosecution of a fraud scheme that made use of computers in several different states, even if its laws were deemed applicable to some of the criminal conduct.

The Administration's proposal tracks the language of the mail and wire fraud statutes as much as possible so that the extensive body of case law that has been developed with respect to these statutes can be applied. In this regard, I would emphasize that we oppose a provision in the computer fraud offense that was passed by the House in the last Congress. That provision would have required the government to prove that the defendant lacked authority to access the computer involved in the crime. Requiring proof of lack of authority makes no sense in

BEST COPY AVAILABLE

cases which involve the use of a computer to divert illegally money or other property. While proof of lack of authority may make considerable sense if the offense is designed to protect privacy interests, computer fraud should be regarded as an economic crime designed to protect property interests, and access authority or the lack thereof is not relevant.

Third, our bill would make it a federal crime, punishable as a felony, to destroy willfully and without authority any computer owned or operated on behalf of the federal government or of a federally insured financial institution, or a computer program or data contained in such a computer. There is a clear federal interest in protecting this limited class of computers from physical destruction and from having the data they contain erased or altered. Such a provision would represent only a very minimal expansion of federal jurisdiction into an area traditionally reserved for the states.

Finally, any new computer crime legislation should contain a criminal forfeiture provision under which the defendant's interest in any computer involved in the unauthorized access offense, the computer fraud offense, or the computer destruction offense could be forfeited to the government on his conviction. Such a provision might prove to be an especially effective deterrent for persons who would use their home or small business computer to make unauthorized access to a government computer. Historically, courts have not given prison sentences or meaningful fines to such persons. In any event, the unauthorized access offense should properly be a misdemeanor. Nevertheless,

BEST COPY AVAILABLE

the prospect of losing an expensive computer could act as a powerful deterrent and serve as a uniquely appropriate punishment for this type of offense.

Mr. Chairman, as I indicated previously, all of the above suggestions are contained in S. 1678, a bill drafted by the Department which Chairman Thurmond introduced and which you co-sponsored. That bill would repeal the provisions in the present section 1030 of title 18 and would make a fresh start in this difficult area. That is the approach we favor but we realize the Subcommittee may decide merely to amend section 1030. If the Subcommittee decides on this approach, I hope that as many of our suggestions as possible will be included. 5/

Mr. Chairman, that concludes my prepared statement and I would be happy to answer any questions at this time.

5/ Another matter that should be included in any revision of section 1030 is a provision stating that nothing in the section is intended to prohibit any duly authorized investigative, protective, or intelligence activity of a state or federal law enforcement agency or of an intelligence agency of the United States. Such a provision is in both S. 1678 and S. 1236, the Department's bill making technical amendments to the Comprehensive Crime Control Act of 1984. A similar exemption was included in 18 U.S.C. 1029, regarding credit card fraud, and also enacted as part of the Comprehensive Crime Control Act. Originally, sections 1029 and 1030 were part of the same House bill and the law enforcement and intelligence exemption, intended to apply to both sections, was inadvertently dropped from the computer crime provision when parts of that bill were added to the Comprehensive Crime Control Act by the House and Senate conference.

BEST COPY AVAILABLE

Senator LAXALT. Senator Trible.

Senator TRIBLE. Mr. Chairman, I have read the complete statement, and I have benefited from your testimony, as usual, Ms. Toensing. I think it is complete and quite helpful, and I have no further questions—at least for the record today. I may well be back in touch on a more informal basis, Mr. Chairman. Thank you.

Senator LAXALT. Very well. As all witnesses know is traditionally the case, there will probably be written questions propounded to various witnesses to be prepared not only by Senator Trible and myself, but also the other members of the subcommittee, and we will get those to you very quickly.

Ms. TOENSING. Thank you, Mr. Chairman.

Senator LAXALT. We thank you very much for your testimony.

Our next witness will be William Petty, who is here representing the National District Attorneys' Association. This gentleman will adequately represent, I am sure, the States rights aspect of this whole issue as a Commonwealth attorney, and having been one myself, or the equivalent thereof in the West, and I know Senator Trible has, you will be speaking to kindred souls.

Senator TRIBLE. Mr. Chairman, if I may interject simply that all Virginians believe passionately in the rights of States, so I am sure that that point of view will be well-represented.

Let me just welcome Mr. Petty and indicate that he serves as the Commonwealth's attorney or prosecuting attorney for Lynchburg, which is a fine community in the south-central part of Virginia, one where I have spent a lot of time. I appreciate Mr. Petty's presence, and I think it adds a sense of the real world which is important to our deliberations here.

Senator LAXALT. We are delighted to have you here, Mr. Prosecutor.

STATEMENT OF WILLIAM G. PETTY, COMMONWEALTH ATTORNEY FOR THE CITY OF LYNCHBURG, VA, ON BEHALF OF NATIONAL DISTRICT ATTORNEYS' ASSOCIATION

Mr. PETTY. Senator Laxalt and Senator Trible, thank you very much for having me. I did enjoy coming up today. It has been some time since I have had the opportunity to drive in Washington's rush-hour traffic. Now I understand why I am in Lynchburg.

You mentioned States rights, and I might just interject that we had a furor in my office not too long ago because we happened to receive a copy of a lawsuit directed at us. We were trying to be tied in with the State, and one of the allegations was that the State of Virginia is a political subdivision of the United States of America. The response we filed was they may have tried to decide that 100 years ago in the War Between the States, but we did not concede then, and we do not concede that issue now. [Laughter.]

Senator LAXALT. Good for you.

Mr. PETTY. Mr. Chairman and Senator Trible, the fact that we are here today discussing this ever-increasing problem of computer-related crime is in itself testimony to the magnitude of this threat. While 50 years ago the machine gun was the instrument of choice of many bank robbers, today it is rapidly becoming the computer. This change has occurred due to the ever-increasing reliance that

BEST COPY AVAILABLE

business and other financial institutions are placing on computers and the increasing sophistication of those who seek to steal from these institutions.

From the storage of sensitive information to the actual transfers of property, businesses have entrusted their computer systems with billions of dollars worth of assets vital to the continued viability of our economy. However, the very capabilities of the computer that make them such a valuable tool of business also allow the knowledgeable but dishonest user to penetrate the most sophisticated security system and access the information within.

Unfortunately, the criminal law has failed to keep pace with these rapid technological advancements. We continue to apply criminal law developed in the 18th century to abilities and technology that never could have been envisioned by jurists of that time.

Senator LAXALT. Does that apply, Mr. Petty, on the State level as well? How are you doing on the State level in Virginia in trying to keep pace?

Mr. PETTY. One of my major concerns in Virginia is the fact that we continue to tie computer fraud to the concept of larceny, and we continue to require the proof of a specific value of the items that are either destroyed or obtained. And I think——

Senator LAXALT. How is that determined? That is a curious element and one that I find hard to understand. How do you tie a value of data——

Mr. PETTY. I think I got personally involved in this as a result of a case I tried about 6 years ago that involved three security salesmen for a local financial institution that took a position with a competing bank, and when they left they took with them, by wrongfully accessing their former employer's computer system, a list of money market securities that were being safekept by their employer. This computer listing contained billions of dollars worth of money market securities, and the testimony was, would have been worth millions of dollars in profits to the competing bank, simply because they would be able to contact those customers when these came up for renewal and the time for trade came up. They spent thousands of dollars purchasing the computer services through which this material was maintained, but the paper that it was printed on itself had absolutely no value. And we ended up trying a 2-week petty larceny trial because the court would not permit us to introduce evidence other than fair market value or proper retail value. And as I mention later in my statement, the very fact that this information is being maintained for confidential purposes precludes it being sold in trade on the open market.

Senator LAXALT. May I ask you a question on jurisdiction? We are talking here—and all of us want to arrive at a result where the lines of jurisdiction are clearly drawn—about Federal activity, Federal jurisdiction, local activity, and local jurisdiction. In the case that you just cited, is that clearly an intrastate activity? Did anybody assert that computer activity of any sort is necessarily interstate in character and could be moved?

Mr. PETTY. This was a completely local situation——

Senator LAXALT. No question about that—no ties elsewhere to——

BEST COPY AVAILABLE

Mr. PETTY. Other than the fact that they were banking institutions and federally regulated by all of the activities——

Senator LAXALT. But that was determined to be purely a local activity.

Mr. PETTY. Yes, sir.

Senator LAXALT. Was that point ever raised by counsel?

Mr. PETTY. No, sir. That was never an issue in the case. It actually could have been tried as an embezzlement or a larceny, but we felt that by doing that, we would not be able to prove that requisite value to make it a felony.

Senator LAXALT. The only reason I raise that is obviously, you know, if you are defending, very often you will shop for an appropriate, more favorable court. It is not unusual to have proceedings commence on a local level, and you say, "Listen, I might do better in the Federal court." But you have not found that to be the case, and in this particular case, you found that to be fairly a local activity and no attempt whatsoever to move it.

Mr. PETTY. Yes, sir. I am not sure you could remove a State prosecution to Federal court. We, under Virginia law, would be precluded from prosecuting once the U.S. Attorney's Office brings it under their jurisdiction.

Senator LAXALT. That is under the doctrine of preemption.

Mr. PETTY. Yes, sir—well, we have a specific statute that even though it might be separate offenses, it could be charged.

Senator LAXALT. So as a practical matter, on the ground where you are, there is no real blurring of jurisdiction. If it is clearly a violation of State statute or appears to be, and there has been no cooption on the part of the Feds, then you can proceed safely on the jurisdictional basis to go ahead.

Mr. PETTY. That case presented that issue. I am very concerned about the kind of case where you have problems not only with interstate, or intergovernmental agency jurisdiction, but also intrastate venue. And as I have mentioned in my statement, in order to prosecute any case, you have to prove that the offense occurred within the jurisdiction of the court. And with computers and the ability to access from ordinary telephone lines, many times it is going to be virtually impossible to prove where an offense occurred.

Virginia's new statute, I think, probably covers that because it includes as one of the elements of venue the residence of the offender, which I think we can establish in any regard. But many States—and Virginia, up until last year—did not address that problem.

I considered that to be a very significant deficiency in our State law.

Senator LAXALT. Very well. Proceed. I hope I have not fouled up your train of thought completely. We get used to that around here; we are rather disjointed.

Mr. PETTY. Speaking as a local prosecutor who has had to deal with the deficiencies of what I consider to be an oversimplistic State law, I would highly recommend to this committee enactment of comprehensive Federal legislation in this area. Present statutes such as those in Virginia present significant difficulties in prosecuting computer fraud.

BEST COPY AVAILABLE

As examples, I would suggest the following. Venue, as I have just mentioned. The unauthorized access to these computers often comes from remote computers through the use of ordinary telephone lines. In addition, a computer system subject to such access might be physically located in several different jurisdictions. Quite often it is difficult, if not impossible, to determine where that unauthorized access occurred. Because proof that the offense occurred in the jurisdiction of prosecution is required, it is conceivable that you not be able to prosecute in any jurisdiction within the State.

Senator LAXALT. Is there a presumption in your statute that access would come from a given place?

Mr. PETTY. The statute lists a variety of criteria that establish venue, and I think probably under the Virginia statute as it now exists, we could, as I say, establish venue in the vast majority of cases. What concerns me are the situations where the computer is spread out, and the access comes from some remote jurisdiction. Even in that case, we might very well have to rely upon something like the residence of the offender, and that many times is difficult to establish.

As I have mentioned, Virginia continues to recognize the concept of computer fraud as larceny. We continue to try to deal with this fraud under common law concepts of larceny. It continues to require proof of value in order to prosecute as a felony. All too often this type of offense deals with the theft of confidential business information. Although the unauthorized use of this information might mean the loss of millions of dollars in profit, it is virtually impossible to put a market value on something that by its very nature is never traded or sold on that open market. In addition, larceny requires proof of an intent to permanently deprive an owner of his property. We run into serious problems when we deal with the theft of information that is duplicated but never actually removed from the computer.

We have inconsistent and inappropriate punishments, in my opinion, in Virginia. Present law makes it a simple misdemeanor to access a computer and tamper with or destroy computer information. The maximum punishment for such an offense is a 12-month jail sentence or a $1,000 fine. Unfortunately, this type of action could result in the loss of information vital to the continued economic life of the company and could give a competitor a significant business advantage.

On the positive side, I see the following benefits to a comprehensive uniform Federal statute dealing with this offense.

Better investigative resources. This type of crime is extremely difficult to detect and prosecute. Very often local law enforcement agencies do not have the level of training and experience to conduct this type of investigation. These local agencies cannot commit the resources needed and still fulfill their obligation of responding to local offenses. In addition, such an investigation may very well involve a number of different law enforcement agencies, often in different States.

Federal legislation would allow a single agency such as the FBI to conduct and coordinate investigations and would make available the resources necessary for a successful prosecution.

BEST COPY AVAILABLE

Senator LAXALT. I hate to do this to you, but we have got five bells on, which means we should go somewhere in a hurry. So let us take a short recess, Senator Trible and I will go over and do our duty and be right back.

Mr. PETTY. Thank you, Mr. Chairman.

[Short recess.]

Senator SPECTER. May I reconvene the hearing just long enough to commend the chairman for calling this hearing. I have obligations elsewhere with the Intelligence Committee.

The hearing will await the return of Senator Laxalt.

We stand in recess again.

[Short recess.]

Senator LAXALT. Please proceed, Mr. Petty.

Mr. PETTY. I was mentioning what I consider to be some of the benefits of a comprehensive uniform Federal statute dealing in this area, and I mentioned problems in investigative resources. I think a similar problem exists in the area of prosecutorial resources.

While the magnitude of this type of offense can be large, it is not the type of offense that most prosecutors will face on a day-to-day basis.

In Virginia, the majority of prosecutors are part time and have a very small, if any, staff. Even though each has within his jurisdiction a potential victim, such as a financial institution, they do not have the experience or the resources to effectively deal with this crime.

By centralizing the prosecution of these offenses within the Department of Justice, I believe a better effort could be made to convict the individuals involved.

Further, the ability of the Department of Justice to prosecute within a single U.S. attorney's office offenses that may involve a number of persons in different jurisdictions would most surely result in higher rates of conviction.

Senator LAXALT. Just being the devil's advocate for a moment, you are talking about resources and needing more horsepower—why can't that be accomplished on the State level as opposed to turning to the Feds?

Mr. PETTY. Speaking only to Virginia which is where I have my experience, the attorney general's office, while theoretically authorized to become involved in the prosecution of criminal offenses, does so very, very rarely. I do not recall it ever happening.

Senator LAXALT. So they do not have State investigative resources that could be helpful to a small area prosecutor?

Mr. PETTY. We do have resources through the Virginia State Police, but again this is not the kind of crime that is going to come up with sufficient frequency that they could afford to maintain the type of staff that is going to be necessary to deal with it.

Finally, I believe that it would benefit all of us to have a uniform definition of criminality. At present, there is no uniform definition of what constitutes criminal conduct in this area. Business and financial institutions no longer are restrained by State boundaries. The information that this type of legislation seeks to protect crosses these boundaries millions of times each day. Business and financial institutions need to be secure in the knowledge that the determination of whether or not a crime has occurred does not

BEST COPY AVAILABLE

depend on the peculiarities of a particular State's law. It is this type of inconsistent treatment that often leads to nonreporting of criminal activity by these businesses.

If we are going to deter this activity, we must have the full cooperation of the victim, and they must have confidence that we can and will obtain convictions no matter where the offender is located.

In addition, we need legislation in this area that is sufficiently flexible to take into account new and increasingly sophisticated ways by which this type of crime may be committed. Too often, State laws are patchwork statutes that address weaknesses only after they have been exposed by the commission of a theft. By utilizing concepts found in Federal wire and mail fraud statutes. I believe that legislation can be drafted that will not be obsolete the day after it is signed into law.

In summation, let me thank you and give you my support for your willingness to address this serious and ever-growing problem. All too often, technological advancements such as computers provide would be criminals with fertile fields in which to plow their criminal enterprises. Hopefully, with the type of support and assistance that this committee has shown, we in law enforcement will be able to raize those fields before they come to fruition.

Thank you.

Senator LAXALT. I thank you in behalf of the members of the subcommittee, Mr. Prosecutor. You have been enormously helpful.

[Statement follows:]

BEST COPY AVAILABLE

STATEMENT OF WILLIAM G. PETTY
COMMONWEALTH'S ATTORNEY FOR THE CITY OF LYNCHBURG

Mr. Chairman and Members of this Committee:

The fact that we are here today discussing the ever increasing problem of computer related crime is in itself testimony to the magnitude of this threat. While fifty years ago the machine gun was the instrument of choice of many bank robbers, today it is rapidly becoming the computer. This change has occurred due to the ever increasing reliance that business and financial institutions are placing on computers and the increasing sophistication of those that seek to steal from those institutions. From the storage of sensitive information to actual transfers of property, businesses have entrusted their computer systems with billions of dollars worth of assets vital to the continued viability of our economy. However, the very capabilities of the computer that make them such a valuable tool of business also allow the knowledgeable but dishonest user to penetrate the most sophisticated security system and access the information within.

Unfortunately, the criminal law has failed to keep pace with these rapid technological advancements. We continue to apply criminal law developed in the Eighteenth Century to abilities and technology that could never have been envisioned by jurists of that century. And when we do consider new legislation to address this problem it all too often comes as a reaction to a specific crime and does not take into account the variety of forms computer fraud can take. It is now time that we take a take a comprehensive look at this Twentieth Century problem and come up with well considered legislation that will give those of us in law enforcement the tools that we need to prosecute and convict those persons who constitute such a threat to our economic system.

Speaking as a local prosecutor who has had to deal with the deficiencies of an overly simplistic state law, I would highly recommend to this Committee enactment of comprehensive federal

BEST COPY AVAILABLE

legislation addressing this area. Present statutes, such as those in Virginia present significant difficulties in prosecuting computer fraud. As examples of these difficulties I would suggest the following:

1. Venue--Unauthorized access to computers often comes from remote computers through the use of ordinary telephone lines. In addition, a computer system subject to such access might be physically located in a several different jurisdictions. Quite often it is difficult if not impossible to determine where the unauthorized access has occurred. Because proof that the offense occurred in the jurisdiction of prosecution is a required element of any offense it is quite conceivable that we would be unable to prosecute an offense of computer fraud in any state jurisdiction.

2. Concept of computer fraud as larceny--Virginia law continues to try to deal with computer fraud under the common law concept of larceny. It continues to require proof of value in order to prosecute as a felony. All too often this type of offense deals with the theft of confidential business information. Although the unauthorized use of this information might mean the loss of millions of dollars in profits, it is virtually impossible to put a market value on something that by its very nature is never traded or sold on the open market. In addition, larceny requires proof of an intent to permanently deprive an owner of his property. We run into a very serious problem when we deal with the theft of information that is duplicated but never removed.

3. Inconsistent and inappropriate punishments--Present Virginia law makes it a simple misdemeanor to access a computer and tamper with or destroy information. The maximum punishment for such an offense is a 12 month jail sentence and a one thousand dollar fine. Unfortunately, this type of action could result in the loss of information

BEST COPY AVAILABLE

vital to the continued economic life of a company and could give a competitor a significant business advantage.

On the positive side I see the following benefits to a comprehensive uniform federal statute dealing with this offense:

1. Better investigative resources--This type of crime is extremely difficult to detect and prosecute. Very often local law enforcement agencies do not have the level of training and experience to conduct the type of investigation necessary to secure an arrest and conviction. These local agencies cannot commit the resources needed and still fulfill their obligation of responding to local offenses. In addition, such an investigation may very well involve a number of different law enforcement agencies often in different states. Federal legislation would allow a single agency such as the FBI to conduct and coordinate an investigation and would make available the resources necessary for a successful prosecution.

2. Better prosecutorial resources--While the magnitude of this type of offense can be large, it is not the type of offense that most prosecutors will face on a day to day basis. In Virginia the majority of prosecutors are part time and have a very small, if any, staff. Even though each has within his jurisdiction a potential victim, such as a financial institution, they do not have the experience or resources to effectively deal with this crime. By centralizing the prosecution of these crimes within the Department of Justice a better effort could be made to convict these individuals. Further, the ability of the Department of Justice to prosecute within a single U. S. Attorney's Office, offenses that may involve a number of persons in different jurisdictions would most surely result in higher rates of conviction.

BEST COPY AVAILABLE

3. A uniform definition of criminality--At present there is no uniform definition of what constitutes criminal conduct. Business and financial institutions no longer are restrained by state boundaries. The information that this type of legislation seeks to protect crosses these boundaries millions of times each day. Business and financial institutions need to be secure in the knowledge that the determination of whether or not a crime has occurred does not depend on the peculiarities of a particular state's law. It is this type of inconsistent treatment that often leads to non-reporting of criminal activity by these businesses. If we are to going to deter this activity we must have the full cooperation of the victims and they must have confidence that we can and will obtain convictions no matter where the offender is located. In addition, we need legislation in this area that is sufficiently flexible to take into account new and increasingly sophisticated ways by which this type of crime may be committed. Too often state laws are patchwork statutes that address weaknesses only after they have been exposed by the commission of a theft. By utilizing concepts found in federal wire and mail fraud statutes I believe that legislation can be drafted that will not be obsolete the day after it is signed into law.

In summation, let me thank you and give you my support for your willingness to address this serious and ever growing problem. All too often technological advancements such as computers provide would be criminals with fertile fields in which to plow their criminal enterprises. Hopefully, with the type of support and assistance such as this Committee has shown, we in law enforcement will be able raze those fields before they come to fruition.

BEST COPY AVAILABLE

Senator LAXALT. Senator Trible.

Senator TRIBLE. Mr. Chairman, just briefly—would it be fair to say that your comments, although they focus on Virginia, extend well beyond Virginia and would apply with equal force to many other States? I would note that Virginia is one of those 38 States that has fashioned a computer criminal statute, and I would imagine that the problems you have enumerated would be widespread.

Mr. PETTY. When I was involved in the case I mentioned previously and was doing research in preparation for that, at that time I found there was very little State legislation in the area of computer fraud, and that was 6 years ago.

Virginia's statute—the particular computer fraud statute we have today—was drafted in response to the case we prosecuted, and the problems that we have had—I think it was pointed out to many business and financial institutions throughout the State that the businesses were not protected.

So I think that the scope of many of these statutes might not be as comprehensive as is going to be needed. Again, I think that we see it time and time again, that the States are responding in this area only after a crime has occurred and has received some public attention. I do not like to see criminals get one free shot at breaking the law.

Senator TRIBLE. Well, that confirms, at least in part, my sense, Mr. Chairman, that the Virginia law is fairly progressive as State laws go in meeting this new kind of criminal activity, and yet it is flawed, and there are very real problems in effective successful prosecution. That would argue for a Federal response, narrowly drafted, appropriately structured, but a Federal response nevertheless.

I thank you.

Thank you, Mr. Chairman.

Senator LAXALT. I assume, Mr. Petty, you are here not only in your local capacity, but also in your capacity as representative of the National District Attorneys' Association?

Mr. PETTY. Yes, I have been asked to speak on their behalf. I might add that in the area of local versus Federal prosecution, I do not mean to say that we do not need to have local statutes dealing with those offenses, because we surely do have cases that are local in nature, and we have cases many times that are small in terms of Federal concerns and U.S. attorney's office concerns, but they decline to prosecute. So I do think we need to have the ability to pick and choose which cases go before which court. But I also believe that the cooperation between the Department of Justice and local prosecutors has been good enough that we can work within that kind of differentiation without getting into territorial squabbles that none of us need and that benefit no one.

Senator TRIBLE. Mr. Chairman, may I add a word very briefly to that point?

Senator LAXALT. Surely.

Senator TRIBLE. I have served as an elected State prosecutor in Virginia, a Commonwealth's attorney, and I have also served as an assistant U.S. attorney, prosecuting a wide range of major felony crimes in the Federal system. It was my experience that there really were no real problems encountered, at least in Virginia, be-

BEST COPY AVAILABLE

tween the State authorities and the Federal authorities in determining who would prosecute cases, and we would very often yield to the State authorities, and there were certain crimes that were large scale or involved a nexus with interstate activity that were obviously crimes that ought to be prosecuted at the Federal level.

So I would like to see us craft a parallel, Federal structure, with provisions that would permit Federal prosecution in appropriate cases, and that would also encourage the States to be more forthcoming in meeting this kind of new criminal conduct.

Thank you, sir.

Senator LAXALT. Very well. We thank you very much.

Mr. PETTY. Thank you, Mr. Chairman.

The CHAIRMAN. Next, we will hear from a panel composed of John J. Sponski, who is the group executive officer of Sovran Bank; Philip M. Walker, general regulatory counsel of GTE; and Norbert J. Kubilus, who is vice president, Educational Testing Service.

Gentlemen, we welcome you, and you may proceed in any order that you can agree upon.

STATEMENT OF A PANEL, INCLUDING JOHN J. SPONSKI, GROUP EXECUTIVE OFFICER, SOVRAN BANK; PHILIP M. WALKER, GENERAL REGULATORY COUNSEL, GTE TELENET INC.; AND NORBERT J. KUBILUS, VICE PRESIDENT, EDUCATIONAL TESTING SERVICE, LAWRENCE TOWNSHIP, NJ

Mr. SPONSKI. Good morning, Mr. Chairman and Senator Trible. My name is John Sponski. I am the group executive officer with Sovran Bank N.A. with responsibility for the operations and data processing group.

Sovran Bank N.A. is headquartered in Richmond, VA. It is the lead bank in Sovran Financial Corp. As of September 30, 1985, the Sovran Financial Corp. had assets of $8.9 billion. Sovran Bank N.A., provides commercial banking and related financial products and services to its customers through a network of 265 branches located in 108 communities in the State of Virginia. Sovran Bank N.A. is a member of the Federal Reserve System, and its deposits, which total $6.8 billion as of September 30, are insured by the Federal Deposit Insurance Corporation.

Senator LAXALT. You have great television ads, too.

Mr. SPONSKI. I am glad to hear that, Senator. I hope we have a couple of customers on the panel this morning.

This morning, I represent not only Sovran Bank N.A., but the members of the Virginia Bankers Association. We strongly support and recommend passage of legislation to discourage and deter unauthorized access to and use of computer systems maintained by financial institutions.

Although some States currently have statutes which provide for fines or imprisonment for those residing in the State who access and use financial institution computer systems without authorization, these measures are inadequate since they do not address incursions into systems originated by intruders outside a State through the use of current telecommunications technology.

Sovran Bank N.A. strongly supports Federal legislation to combat the risks of exposure to loss from unauthorized incursions

BEST COPY AVAILABLE

into our computer systems by an increasing number of people who have the knowledge and access to technology.

Simple and effective legislation is needed today to discourage and punish unauthorized incursions, particularly when initiated beyond a State's boundaries.

I am confident that the members of this committee appreciate the importance to the financial industry of computers and information data bases. Most of the products and services provided by commercial banks and other financial services companies could not be provided without computers and information data bases. Today, many within the banking industry consider our basic function to be information transfer to our customers rather than depository lending services.

Through the information stored in our data bases, we are able to provide customers with timely, reliable information on their financial condition so they in turn can transfer funds with confidence and invest wisely.

Today the value to a bank of the information stored in its data bases far exceeds the value of its vault cash. Frankly, information is more valuable than cash because it has far greater potential for use.

Senator LAXALT. How is that listed on your statement?

Mr. SPONSKI. It is not listed, Senator. We have a very difficult time trying to place an absolute value on information.

Senator LAXALT. So if Sovran wanted to structure a financial statement, the value of your data base is not included at all, even though you indicate the value of that is more than your cash.

Mr. SPONSKI. It has value, depending upon the way it is being used.

Senator LAXALT. Why is that? Why haven't accounting procedures proceeded to the point that you could value that?

Mr. SPONSKI. That is a problem that has confronted us in attempting to prosecute cases where there have been incursions into systems, because the courts keep on insisting: "Define the value of the information." And the value is implicit in the information, based upon the way it is used.

Senator LAXALT. Well, why can't the banks get together and solve that problem, and establish criteria for establishing a value and listing it?

Mr. SPONSKI. Because under current accounting practices, there is no standard way to value information.

Senator LAXALT. I understand that. But why don't they get together and establish standards under valid accounting procedures? Is that just impractical, or what?

Mr. SPONSKI. I think an easy answer to your question is that the rate of progress in technology and the use of computers has gone faster than we have thought of the implications of their use.

Senator LAXALT. That is probably where it is, all right.

Mr. SPONSKI. The information data bases meet our customers' financial services needs. We analyze data for marketing strategies and programs. We provide various reports to regulatory and Government agencies, and of course, we maintain our own corporate records.

BEST COPY AVAILABLE

Banking today cannot function without timely, accurate, and detailed information data bases.

Sovran Bank's use of and reliance on computers reflects the prevalent condition in the banking industry. The Sovran Financial Corp. currently has slightly more than 8,000 employees. We have 5,500 terminals connected to our computers. These devices are used by our employees and our customers. Daily, over 750,000 transactions or requests for information are entered through these terminals. At present, Sovran has 172.8 billion bytes of data stored on our disk units. If we were to print out this data on computer paper with 7,500 characters per page, this would result in a report 3,271 miles long—the distance from San Diego, CA, to Acadia, ME.

The information we have on our computer systems is proprietary in the sense that it is ours, obtained from our customers to meet their financial services needs. This information is also private, since it is about our customers and that most confidential subject—their money. In this regard, the information has been entrusted to us.

Now, recognizing our responsibility to safeguard this valuable asset information, Sovran and other banks have in place various means to control access to our information data bases. At Sovran, we employ a series of progressively restrictive access control methods. These measures include restricting access to data bases to only those employees who must use the information to service customers; requiring unique access codes assigned to each terminal user to identify and monitor entry to the data base, requiring frequent changing of access codes; protecting application systems with highly structured terminal control systems which limit the use of terminals to specific individuals by function, by type of transaction, and other criteria, by employing dial-jack techniques for systems accessibility to dial up terminals, and lastly, selective use of message authentication or encryption of data.

These are elaborate and expensive measures we have taken to protect this valuable asset, information. But the true value in information is its use. Consequently, control systems, no matter how effective, must permit access to the information for use.

The most effective vault is one with floors, walls, and ceiling made of thick, reinforced concrete. This vault also is elaborately alarmed to detect attempted intrusions, and, to guarantee security over the stored valuables, there is no door.

No door means no access. No opportunity to bypass the alarms and the thickly constructed walls, floor, and ceiling. Information stored in a data base in such a way that it cannot be accessed is indeed secure, but it is also, frankly, useless and valueless.

Sovran Bank and most users of computer information have installed reasonably effective and practical safeguards. But the rapid advances of technology, the extensive development of telecommunications systems, and the ready availability of powerful microprocessors, together with the growing knowledge and experience of many within our Nation about computer systems, are eroding our safeguards.

Computer hacking is an intellectual challenge for many. For those so inclined, it has replaced the intricate strategies and thought processes of a chess game. This interest in beating an

BEST COPY AVAILABLE

access control system will not diminish so long as the intruders receive notoriety in the media and a verbal reprimand cautioning them to put their talent to other applications.

In 1984, the Computer Crime Task Force of the American Bar Association surveyed 1,000 private organizations concerning the nature and occurrence of computer-related crime. Seventy-nine percent of the respondents indicated support for a Federal criminal statute as needed to combat unauthorized intrusions into computer systems. Sovran Bank N.A. and the Virginia Bankers Association are also strongly in support of a Federal statute which would deal with intrusions occurring both intra- and inter-state. Intruders are not limited by State boundaries.

Low-cost, long-distance telephone systems permit the intruders to make their gambit at a most reasonable cost.

A Federal statute imposing strict fines and imprisonment terms would complement the efforts taken to date and planned by Sovran Bank N.A. and other financial institutions to protect and control access to data.

But since we must put that vault door on our perfect vault, so also must access be allowed to our information systems. And just as it is a violation of a Federal statute to rob the vault of a bank, we believe it should also be a violation of a Federal statute to gain entry without authorization to an information data base, or to misuse an information data base when access is authorized, and most certainly, when data is altered, added or deleted within an information data base by an unauthorized user.

Without a Federal statute to discourage unauthorized entry into information data bases, any measures or techniques will be countered, like in chess, by the skillful, talented, and highly intelligent intruder or hacker.

Of course, existing Federal statutes have not eliminated bank robberies, but these statutes have definitely discouraged a casual attitude toward robbing a bank. A Federal statute which requires the intervention of Federal investigative agencies into incidents of unauthorized access to and misuse of information data files will not eliminate every occurrence, but it will certainly increase the penalty of the game.

Mr. Chairman, Senator Trible, we know you must consider and evaluate many requested Federal statutes, but we earnestly request you to act speedily to pass legislation to provide another measure of protection to the vital information data bases and computer systems, both in existence and under development in our progressively technologically developed nation.

Thank you for the opportunity this morning to present the concerns and recommendations of both Sovran Bank, N.A., and the Virginia Bankers Association.

Senator LAXALT. We thank you, Mr. Sponski. You expressed those concerns very well.

Senator Trible.

Senator TRIBLE. Good statement, and I thank you for being here this morning and speaking not only in behalf of Sovran, but also all the banks and financial institutions in Virginia.

I have no questions, Mr. Chairman.

Senator LAXALT. Very well. Who is next?

BEST COPY AVAILABLE

STATEMENT OF PHILIP M. WALKER

Mr. WALKER. Mr. Chairman, good morning.

I am Philip Walker, general regulatory counsel for GTE Telenet Inc., based in Reston, VA.

I would like to thank you for the opportunity to share with you some of Telenet's views on Federal legislation regarding computer crime.

GTE Telenet is one of the Nation's leading providers of packet switched data communication services and electronic mail services. We also provide specialized computer-based services oriented toward particular fields, such as securities brokerage and the medical profession. GTE Telenet also furnishes credit verification and point-of-sale transaction processing services for the retailing industry.

Telenet's nationwide data communications network serves approximately 2,000 data base and data processing computers, almost all of which are owned and operated by our customers. Hundreds of thousands of terminal users dial into this network daily from every State in the Union and from more than 65 overseas countries, to access information in computer data bases, to send electronic messages, to process transactions, and the like.

Telenet and its customers have taken a variety of technical and administrative steps to prevent unauthorized access to these computer systems, and Telenet is in the forefront of innovative developments in the data network security field. Nonetheless, there have been a number of widely publicized incidents of unauthorized penetration of various computers on the Telenet network, as well as penetration of computers on other competing data communications networks. The subcommittee is undoubtedly familiar with some of these incidents, and I will not take the time to detail them here.

Suffice it to say that the advent of efficient, low-cost data communications capabilities such as Telenet's public network service, has not only provided enormous benefits to society in making computing capabilities more widely available, but has also contributed to a substantial increase in computer crime.

Some of these incidents have been the work of the stereotypical young hacker, interested more in beating the system than in malice of theft. However, an alarming number have involved adults rather than teenagers and have involved malicious damage to computer files, theft of valuable information and even, in at least one case, potential jeopardy to human life.

In Telenet's view, comprehensive Federal legislation on computer crime is urgently needed. First, computer crime is increasingly interstate in nature. At the touch of a few keys on his computer keyboard, an offender located in one State can use data communications network facilities to access computer systems located not only in his own State, but also in numerous other States around the country. Often, the offender does not even know, or care, where the computer is located that he is attempting to penetrate. No State statute and no local prosecutor can adequately cope with this situation.

BEST COPY AVAILABLE

Second, in our view, effective law enforcement in this area requires uniformity of legal protection across the country. While a number of States have enacted various computer crime statutes, one-third have no such laws on their books. Moreover, the State laws which do exist are a "crazy quilt" of inconsistent provisions, differing widely from one State to the next in terms of what types of computer systems are protected, what types of offenses are covered, what penalties may be imposed and the like.

Certainly, there is a legitimate State interest in deterring and punishing computer crime of a purely intrastate nature. We believe, however, that there is an equally important Federal interest in computer crime which takes place across State lines, which affects interstate or foreign commerce, or which uses interstate telecommunications facilities.

Mr. Chairman, in preparing for this hearing, we have reviewed Senator Trible's bill, S. 440, and I would like to comment on several aspects of this bill. First, I wish to emphasize Telenet's support of this important legislation.

I will focus this morning on two aspects of S. 440: First, the scope of Federal jurisdiction as defined by the bill, and second, the offenses covered by the bill and the penalties provided.

With respect to Federal jurisdiction, S. 440 recognizes both the Federal and State interest in computer crime, and balances these interests. On the one hand, it provides for Federal jurisdiction over an offense if the target computer "operates in or uses a facility of interstate or foreign commerce." This provision brings within the bill's protection all of the computer systems connected to Telenet's nationwide telecommunications network, and thereby provides the uniform protection which we believe is needed.

On the other hand, S. 440 recognizes that this Federal jurisdiction may exist concurrently with State or local jurisdiction over a particular offense, and the bill admonishes Federal law enforcement officers to consider a number of factors in determining whether to exercise Federal jurisdiction. This approach, we believe, offers the benefits of a uniform Federal statute but preserves the authority of State and local officials to prosecute crimes that fall more appropriately within their jurisdiction, assuming they have the necessary statutory tools.

It is our understanding that the subcommittee is also considering an alternative approach to Federal computer crime legislation. Under this approach, Federal jurisdiction would exist only if the offender and the target computer are located in different States—except for computers operated by the Federal Government or a financial institution—irrespective of whether the target computer operates in interstate or foreign commerce, or whether the offense involves the use of interstate telecommunications facilities. This approach, we feel, would create an unnecessary gap in an otherwise uniform structure of legal protection for computer systems.

As I have noted, nationwide public data telecommunications networks such as the Telenet network, are increasingly used by computer systems operators to provide remote access to their systems. In such networks, the distinction between "interstate" and "intrastate" telecommunications often loses its meaning. For example, Telenet operates a financial database service called Finet, which

BEST COPY AVAILABLE

utilizes computer facilities located in Reston, VA. These computers are connected to our nationwide packet-switching network, which offers dial-in telephone access for terminal users throughout the country.

But suppose an individual located only a few miles away, in Alexandria, VA, seeks to penetrate the Finet system. He would connect his personal computer to his telephone and dial the local Telenet access number to reach the Finet host computer. However, this would not be an intrastate activity, even though both Alexandria and Reston are within the Commonwealth of Virginia, for the Telenet network node which serves Alexandria is located in downtown Washington, DC. Thus, the offender would place an interstate telephone call in order to reach the network access node. Further, once he reached the access node, depending on network congestion at that particular instant, traffic from Washington to Reston might be routed by the network through yet a third jurisdiction.

In our view, criminal activity of this sort should be subject to Federal jurisdiction. This is akin to Federal laws which prohibit wiretapping and wire fraud which may occur solely within a single State, but which involve interstate telecommunications facilities.

Let me turn briefly to the substantive content of S. 440. Unlike the computer crime bill passed by the Congress last year, this bill is not limited to any particular class of computer systems, such as Federal Government computers or computers operated by financial institutions. Rather, and much to its credit, it would appear to cover virtually any computer in the private sector as well as the public sector, provided the jurisdictional requirements are met.

Our industry sorely needs this broad protection.

Additionally, S. 440 defines a two-tier hierarchy of offenses, beginning with a misdemeanor offense for simple trespass—that is, accessing a computer knowingly and without authorization. At the second tier, a felony offense is created for various acts which go beyond mere unauthorized access, such as use of the computer to defraud or steal, or to damage or destroy property—including information and software contained within the computer itself—we believe this two-tier structure is appropriate, and we commend its inclusion in the bill.

On the other hand, this bill does not provide for civil penalties to compensate victims for the destruction or theft of property. Civil penalties, particularly in the form of double or treble damages, and statutory minimum damages, would provide such monetary redress for victims of computer crime. Addition of such provisions to the bill would also enable victims to act as "private attorneys general," thereby complementing the efforts of law enforcement agencies.

Law enforcement officials are often overburdened with the investigation and prosecution of more serious crimes, and may have insufficient resources to pursue a particular computer offense Also, in some cases, although there may be insufficient evidence to obtain a criminal conviction, a civil lawsuit—with its lower burden of proof—might succeed if a cause of action were provided in the Federal legislation.

In this connection, I would note a bill recently introduced by Senator Leahy and Representative Kastenmeier—S. 1667/H.R. 3378—entitled the "Electronic Communications Privacy Act of

BEST COPY

1985." This bill provides protections for telecommunications privacy, including electronic messages stored in computers during transit, that are essentially complementary to the computer crime provisions of S. 440.

I recently had the pleasure of testifying in support of that bill before Representative Kastenmeier's House Subcommittee, on behalf of the Electronic Mail Association. I mention that bill here for two reasons. First, we believe that both the Leahy/Kastenmeier bill and a comprehensive computer crime bill such as S. 440 are needed. Neither alone provides the full scope of protection for computer and telecommunications systems. Second, the Leahy/Kastenmeier bill illustrates how both civil and criminal provisions can be incorporated into legislation dealing with this area. I would suggest this concept for your consideration in any revision of S. 440.

Mr. Chairman, in summary, this legislation represents an important and valuable response to the growing computer crime problem. GTE Telenet particularly applauds its jurisdictional breadth, its scope of coverage, and its treatment of various levels of offenses. We suggest, however, that civil provisions also be considered for inclusion.

Thank you for the opportunity to present our views.

Senator LAXALT. We thank you, Mr. Walker, and we thank you particularly for your suggestion in connection with the civil penalties. That is something that has been raised from time to time, but I think that you have justified it very well in your statement.

Senator Trible.

Senator TRIBLE. Mr. Chairman, let me simply thank Mr. Walker for a very fine statement and for some very valid recommendations.

Let me simply observe that your testimony underscores the fact that information today knows no boundaries; that computer networks reach far and wide, and it is important for us as we struggle to shape the definition of the required Federal nexus or interstate quality of crimes, that we respond to that reality. That is not easy, but I think you have underscored the reality of technology today, and we will be guided by your good advice and counsel.

Thank you, Mr. Chairman.

Senator LAXALT. Very well, then; Mr. Kubilus, will you sum up?

STATEMENT OF NORBERT J. KUBILUS

Mr. KUBILUS. Thank you, Mr. Chairman.

My name is Norbert J. Kubilus, and I am vice president for information systems and technology at Educational Testing Service.

I am here today by your invitation to state ETS's strong support for enacting computer crime legislation that would adequately protect computers in the private sector against unauthorized intrusions, fraud and outright abuse.

I have submitted a fairly lengthy written statement, and I will take this time to summarize some of the high points of it and to focus on some of the issues.

ETS spends over $7 million a year on test and computer security. Despite this investment and the protection it furnishes, existing

BEST COPY AVAILABLE

laws, both State and Federal, provide little legal deterrent to hackers and others who attempt to breach computer security.

ETS's computers, like most other private sector computers that are used in interstate commerce, or, in some cases, for the benefit of the Federal Government, are not protected by existing Federal law. The Federal Computer Systems Protection Act of 1985 would be a welcome legal deterrent to hackers and others who attempt unauthorized access or use of our computers.

ETS develops and maintains testing programs in the United States and overseas. Our computers reside in various States in the United States, and we use interstate electronic communications facilities, including those of Telenet. Some of the services that we provide are for the benefit of the Federal Government. The Department of Defense, Department of State, Department of Education, and others outlined in my written statement rely on computer based or computer—assisted services provided by ETS.

Recently, ETS has announced a commitment of $30 million to develop new testing forms through the end of this century and into the next century, most of which are going to be based on computer and other technologies. Without the computer, the kinds of advances that ETS is making in new approaches to testing and test administration for the benefit of examinees and those who use these test scores, would be impossible.

But as the others have also noted this morning, the computer opens new opportunities for theft and damage of proprietary and confidential information.

Securing these computers and information on them is our management concern. Effective deterrrence of efforts to tamper with them, and/or misappropriate information requires comprehensive and properly stringent computer crime legislation.

With the shift from paper and pencil tests to tests delivered electronically, often over communications lines, copyright protection alone is insufficient and existing laws ineffective in coping with electronic trespass. ETS encourages passage of Federal computer crime legislation that has several characteristics to it. First, that it covers computer trespass across State lines—S. 440 does that. Second, that it recognizes that the object of computer crimes can be the information produced by or maintained on the computer, and both bills do that. Third, that effective legislation should define both civil and criminal remedies. As has already been mentioned, they both provide for criminal remedies, but do not provide for injunctive relief or damages.

Both bills provide for misdemeanor and felony penalties, but the financial felony penalty in S. 440 is about one-fifth of that in S. 1678. ETS would strongly urge adoption of the higher ceiling on monetary penalties at $250,000.

This penalty ceiling would give indication of the seriousness of the offense. In our case, where it costs us hundreds and hundreds of thousands of dollars to develop a test, to have that test stolen electronically to benefit somebody else who does not have to spend that money, a $250,000 fine would be more commensurate with the loss.

Fourth, that the legislation provide maximum technical guidance for prosecutors and judges. Here, we see a difference between the

BEST COPY AVAILABLE

two bills. In the administration's proposed legislation, we find a comprehensive set of definitions of technical terms. In fact, it also fits another criterion that we have, that this legislation anticipate computer crime involving new or emerging technologies. For example, the administration's bill refers to optical storage and other forms of new technology.

We also encourage that Federal legislation avoid using a financial value threshold to delineate between Federal and State jurisdiction. The value of the information—as you have heard, Mr. Chairman, in responses to your questions this morning—is hard to compute or assess. We can place a value on what it costs to collect that information or what it would take to reproduce it, but the ultimate value of stolen information is often hard to determine.

S. 1678 meets most of our requirements, and we would encourage its passage with the changes I have suggested.

Let me point out some of the far-reaching effects of that bill that ETS views positively. In moving toward electronic testing medium, ETS is already using the computer to produce, generate and publish testing materials. The administration's bill would make theft of these tests a criminal offense, in that our computers are used for the benefit of the Federal Government.

We are also involved in developing, electronic means of testing. It would appear that the administration's bill could open the door to allow us to prosecute, under the proposed legislation, the fraudulent use of computer based testing, especially cases involving test impersonators.

As you may be aware, recently ETS cooperated with the Immigration and Naturalization Service in the investigation of individuals who were using falsified passports to gain admission to tests that ETS administers. Results of these tests are then used to obtain visas for foreign nationals to attend universities in the United States.

I raise these questions and comments in my prepared statement not as weaknesses in the proposed legislation, but rather to help to focus on some of the issues and some need for clarification.

To sum up, an individual who breaks and enters a computer, whether that be a hacker, a common electronic thief, or someone who is looking for information for personal or financial gain, violates the rights and privacies of the authorized users of that computer system.

At ETS, our computer files contain confidential and proprietary information about test sponsors, test candidates, institutions and the tests themselves. ETS will continue to be vigilant in our observation of computer security procedures and our adaptation of those procedures to security needs as they evolve, as the technology evolves.

ETS supports passage of the Federal Computer Systems Protection Act of 1985, with the changes I have suggested, and I hope my testimony today will help facilitate that enactment.

I thank you, Mr. Chairman, for the privilege of appearing here today, and I will be glad to respond to any questions you may have.

[Statement follows:]

BEST COPY AVAILABLE

TESTIMONY BEFORE
THE SUBCOMMITTEE ON CRIMINAL LAW
OF THE COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

by

Norbert J. Kubilus
Vice President
Educational Testing Service

Mr. Chairman. Members of the Subcommittee on Criminal Law. My name is Norbert J. Kubilus, and I am Vice President for Information Systems & Technology at Educational Testing Service (ETS), which has its corporate headquarters in Lawrence Township, New Jersey. I am here today, by your invitation, to state ETS's strong support for enacting computer crime legislation that would adequately protect computers in the private sector against unauthorized intrusions, fraud and outright abuse.

Security Alone Doesn't Afford Absolute Protection

Both in fact and in fiction, ETS is a target for individuals who attempt to bypass our security mechanisms for fun, personal gain and/or commercial profit. ETS spends over $7 million a year on test and computer security. Despite this investment and the protection it furnishes, existing laws provide little legal deterrent to hackers and others who attempt to breach computer security. Secure test questions find their way into test preparation materials published by third parties, individuals offer their services publicly to impersonate test candidates, and electronic intruders (or "hackers") openly attempt to gain unauthorized access to our computers.

In part, these hackers receive encouragement from novels such as **Poker Game** by Fletcher Knebel that give a false impression of the ease with which someone can enter an ETS computer. Electronic joy rides by teenagers such as those in the Milwaukee area who called themselves the "414s" have raised the computer hacker to the level of cult hero. The assumption, however, that most computer hackers are teenagers going through some rite of passage has helped inhibit support of effective computer crime legislation.

Less than forty states have enacted computer crime statutes, and existing Federal statutes have serious limitations. The Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 (Public Law

BEST COPY AVAILABLE

98-473) covers only unauthorized access to computers used by the Federal government, banks, security dealers, and credit bureaus. It does not apply to most private sector computers -- such as those operated by ETS -- that are used in interstate commerce or for the benefit of the Federal government.

The Federal Computer Systems Protection Act of 1985 (S.1678) and the Computer Systems Protection Act of 1985 (S.440) being considered by this Subcommittee would provide additional legal deterrent to hackers and others who attempt unauthorized access and/or unauthorized alteration or destruction of ETS computers or information contained on them.

ETS Role in an Information Society

ETS was founded by the American Council on Education, the Carnegie Foundation for the Advancement of Teaching, and the College Board, and chartered as a nonprofit corporation in December 1947 under the education law of the State of New York. The primary aim of ETS is to serve education through measurement, related services, and research. It develops information systems to assess human talent and provide information for use in planning transitions in individual academic and professional careers, relying on computer and other technologies for collecting, generating and maintaining this information.

As an international leader in measurement and research, ETS develops and conducts many testing programs throughout the United States and overseas. In addition to well-known national programs for academic selection at the high school, college, graduate, and professional levels, it conducts more than fifty programs in career and occupational assessment. **ETS TODAY** describes these testing programs, as well as our research, development and other service activities; I have provided copies of this publication for the members of the Subcommittee. Descriptions of selected Federal contracts with ETS are attached.

ETS operates computer centers in New Jersey, California and Illinois, electronically transfers information among its offices in the United States and Puerto Rico, and uses data communications capabilities through Telenet and regulated other facilities for delivering information and testing services.

Growing Computer Use for Testing

Over ten million Americans take standardized tests each year. For half a century, standardized testing has not changed substantially in its general form -- that is, multiple choice tests with answers recorded using a number 2 pencil on a machine-scorable answer sheet. The integrity of these test scores is vital to admissions officers, certification bodies, licensing agencies, test takers, and others.

BEST COPY AVAILABLE

The ETS Board of Trustees has committed $30 million to develop a new generation of tests. Capitalizing on advances in measurement research and technology, these new tests will be primarily computer-based rather than dependent solely on present paper and pencil methods. Without the computer, the kinds of advances ETS is making in new approaches to testing and test administration for the benefit of examinees and those who use test scores would be impossible.

But the computer opens new opportunities for theft and damage of proprietary and confidential information. Securing these computers and the information on them is a management concern; effective deterrence of efforts to tamper with them or misappropriate this information requires comprehensive and properly stringent computer crime legislation.

ETS Position on Computer Crime Legislation

In the traditional testing environment, the mechanisms for securing tests and test scores are straightforward and dependent on people. Legal protection is in the form of copyright obtained for test materials and existing laws proscribing trespass, breaking and entering, burglary, and so on. With the shift from paper and pencil tests to tests delivered electronically, often over communications lines, copyright protection alone is insufficient, and present laws are ineffective in coping with electronic intruders.

ETS encourages passage of Federal computer crime legislation that:

- covers computer trespass across state lines;
- recognizes that the object of computer crimes can be information produced by or maintained on a computer;
- defines both civil and criminal remedies;
- provides maximum technical guidance for prosecutors and judges;
- avoids using a financial value threshold to delineate between Federal and state jurisdiction;
- anticipates computer crime involving new or emerging technologies.

Computer Trespass. Both S.1678 and S.440 proscribe unauthorized attempts at computer access. Only S.440, however, covers trespass upon <u>any</u> computer that "operates in, or uses a facility of, interstate or foreign commerce." Making such computer trespass a Federal misdemeanor is an important omission in S.1678.

Information as an Object of Crime. Both S.1678 and S.440 recognize that computer-based <u>information</u> <u>is property</u> and has value. I

BEST COPY AVAILABLE

have already mentioned the importance of test security to ETS, and alluded to the increased exposure test materials have in an electronic testing environment. As part of its test development process, ETS uses word processing software to create and edit test items, stores these items as computer-based information, and electronically processes them into human readable forms. ETS would benefit if theft of these computer-generated tests is proscribed as a criminal offense.

Civil Remedies. Neither proposed Act provides for civil remedies. ETS feels that comprehensive computer crime legislation should include the ability to enjoin computer intruders and to obtain damages and litigation costs. The provision for recovery of civil damages along the lines of that included in H.R. 3378 (Electronic Communications Privacy Act of 1985) would be acceptable in any computer crime legislation.

Criminal Penalties. Both S.1678 and S.440 provide criminal penalties. The fines specified in S.440, however, are too low when compared to the possible value of information that may be stolen, modified or destroyed. While it is often difficult to place an absolute financial value on information, there is an investment in creating, collecting and assembling information, there is a cost in reconstructing damaged information, and there is potential lost revenue due to misappropriation of information. The maximum penalties included in S.1678 are more commensurate with the seriousness of computer crime.

Technical Guidance. Both S.1678 and S.440 provide definitions of technical terms, but ETS favors the more explicit definitions given in S.1678.

Financial Value Threshold. Neither bill uses a financial value to trigger Federal jurisdiction.

Anticipating Technologies. Three current or prospective uses of computers by ETS raise questions about the scope of the proposed legislation.

- Computer systems used for computer-based training and computer-based testing involve the integration of audio and video technologies with a computer. It is unclear whether either bill would apply if someone gained access by stealing an audio track or if someone altered a video sequence.

- ETS is introducing a specialized computer system for testing called Keyway. Statewide testing of insurance license candidates using Keyway began earlier this month in Illinois. Nevada and Colorado are the next states where Keyway will be used for insurance license testing. The components of the Keyway system are unconnected at a test center, but the scoring component of the Keyway system communicates electronically with a computer

BEST COPY AVAILABLE

system in New Jersey. It would appear that fraudulent use of Keyway -- such as impersonating a test candidate -- could be prosecuted under S.1678.

- ETS transmits test score reports, financial aid need analyses, and test items electronically to computers in different states. While these computers are connected to ETS, it appears that the provisions of S.1678 apply to the receiving computers. But the connection ceases after the transmission, and the local computer is again a standalone system. It is unclear whether the information sent by ETS to that computer remains protected under the provisions of either bill.

I hope that these questions may help focus on some possible clarifications that may be needed, as well as indicate the far-reaching effects of S.1678 that ETS views positively.

Summary

Dr. Sherry Turkle, in her book **The Second Self** , finds that "in the hacker, people see someone who holds a key to the mysteries [of computers] and is willing to defy the establishment to open them; there is the fantasy of an electronic Robin Hood." Whether the individual on a personal computer on the other end of a telephone line attempting to break and enter a computer system is a hacker, a common electronic thief, or someone looking for personal or financial gain from fraudulent manipulation of information, the result is the same. The rights and privacy of authorized users of that computer system have been violated.

For ETS, computer security issues and the need for effective computer crime legislation go beyond any fear of accidental damage to information. Computer files contain confidential and proprietary information about test sponsors, test candidates, institutions and tests themselves. ETS will continue to be vigilant in our observation of computer security procedures and our adaptation of these procedures to potentially new security needs. ETS supports passage of the Federal Computer Systems Protection Act of 1985 with the changes recommended above, and I hope my testimony today helps facilitate enactment of comprehensive Federal computer crime legislation in the 99th Congress.

I thank you, Mr. Chairman and, through you, your colleagues on the Subcommittee for the privilege of appearing before you today. I shall be glad to respond to your questions.

BEST COPY AVAILABLE

ATTACHMENT

Selected ETS Contracts with the Federal Government

- Since 1955, the Central Intelligence Agency (CIA) has contracted with ETS to set up test centers and administer the Professional Applicant Test Battery for candidates for CIA employment.

- The National Security Agency (NSA) has contracted with ETS since 1968 to provide administrative services for its Professional Qualification Test, which is given each fall to applicants for NSA employment. Also, in 1982, we were asked to collect job performance data to be used as criteria for validation of the NSA Career Qualifications Test Battery, which is used for advancement within NSA, and perform a validation study of the Battery.

- For the Department of State, ETS provides ongoing test development, administration and scoring services for the Foreign Service Officers' examination.

- The Department of Defense contracts with ETS to make DANTES Subject Standardized Tests (DSSTs) and CLEP tests available to the military for college credit. ETS services include developing and distributing the examinations, scoring and reporting the results, and maintaining transcript and inquiry services.

- Also for the Department of Defense, ETS develops the marketing plan, brochure, and student workbook for the Armed Services Vocational Aptitude Battery (ASVAB 14) and provides final forms of the tests as well as assessment reports.

- Under contract to the Naval Supply Center, ETS is currently revising the United States Navy and Marine Corps Aviation Selection Test for pilots and naval flight officer candidates. The test battery will be designed to predict a candidate's performance in training, and will be used as part of the selection procedure for pilots and naval flight officers.

- The ERIC Clearinghouse on Tests, Measurement, and Evaluation (ERIC/TM), funded by the National Institute of Education (NIE), is one of sixteen clearinghouses in the Educational Resources Information Center system. The Clearinghouse collects, evaluates, processes and disseminates information in five areas of interest: tests and information about tests, all types of measurement techniques, evaluation procedures and theory, research methodology, and human development and learning theory.

- National Assessment of Educational Progress (NAEP) is a five year program funded by NIE to assess by means of nationally representative samples the learning of secondary school students and to report its findings to the nation's decision-makers, who will use the information to review and revise educational priorities, policies and practices in schools and at state levels.

- For the United States Peace Corps, ETS conducts a certification and recertification program on in-country staff who administer oral language proficiency interviews in languages other than English. Under this contract, ETS is also developing a prototype of a new oral assessment procedure.

- The United States Department of Education contracts with ETS to provide technical assistance in program evaluation to state agencies and local school districts in the Atlantic coast states from New York to Virginia and in eleven southern states (Regions 1 and 3).

- ETS administers the Presidential Scholars Program on behalf of the Commission on Presidential Scholars and the United States Department of Education. This program seeks to identify and recognize 141 graduating high school seniors for their outstanding accomplishments. Scholars are invited to Washington for a week-long learning experience and are honored by the President.

BEST COPY AVAILABLE

Senator LAXALT. We thank you for an excellent statement.

Senator Trible.

Senator TRIBLE. Mr. Chairman, let me simply conclude by saying that I think this hearing and the testimony we have heard have been quite instructive, and I want to thank you for your leadership and for your taking the time to investigate this matter.

Senator LAXALT. I want to thank you for helping me on the hearings. You have been enormously helpful.

I thank the panelists. I think their statements have been obviously the product of a lot of hard work, and a lot of thought and deliberation. We will make certain that the statements are brought to the attention of the other members of the subcommittee.

We thank you all, and the subcommittee will stand in recess.

[Whereupon, at 11:45 a.m., the subcommittee was adjourned.]

O

BEST COPY AVAILABLE